



# NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

## Operate Within Interconnection Operating Limits Standard Drafting Team Meeting

Tuesday, July 20, 2004, 8 a.m.–5 p.m.

Hyatt Regency Vancouver  
655 Burrard Street  
Vancouver, BC V6C 2R7  
Telephone: (604) 683-1234

Dial-In Participation  
(816) 650-0669  
Access Code: 831018#

### AGENDA

#### 1. Administrative

- a. Membership and Guests — Chair
- b. Introductions — Chair
- c. Organization, Roster, and Survey Contacts List — Secretary (**Attachment 1**)
- d. Arrangements — Lunch on Tuesday July 20, 2004 — Secretary
- e. Parliamentary and Anti-Trust Procedures
  - i. Parliamentary Procedures — Chair (**Attachment 2**)
  - ii. Anti-Trust Compliance Guidelines — Chair (**Attachment 3**)

#### 2. Operate Within Interconnection Reliability Operating Limits Standard Draft, Version 4

- a. Standard Drafting Team to Assess and Re-evaluate IROL Standard Direction  
**Status:** The IROL drafting team identified a potential conflict with the Determine Facility Ratings Standard – and is exploring options available to move the standard forward. Either the definition of an IROL must be revised, or the requirements for establishing System Operating Limits (contained in Requirement 603 of the Determine Facility Ratings Standard) must be modified.
  - b. Consider Original SAR Language — Is it Still Applicable
  - c. Consider Combining this Standard with the SOL Effort
  - d. Consider Changing Scope of Standard to Address Transfer Capabilities instead of SOLs
    - i. Change the name to Monitor and Operate Within Interconnection Operating Transfer Capability Limits
  - e. Change Standard Scope to Include All SOLs
  - f. Address SOLs that impact more than one TOP
  - g. Address SOLs that impact more than one RA
  - h. Convince the DFR SDT to Modify the Language in Requirement 603
  - i. Other Options

- b. Protection of the Transmission System — Concern Raised During BRD SDT WebEx Meeting
  - a. Review BRD SDT White Paper (will be distributed to IROL SDT later)
- c. Review
  - a. Standard 200 Operate Within Interconnection Reliability Operating Limits (**Attachment 4**)
  - b. Implementation Plan (**Attachment 5**)
  - c. Questions & Answers (**Attachment 6**)

### **3. Operate Within System Operating Limits SAR**

- a. SAR Submitted into Standards Process (**Attachment 7**)

### **4. Future Meetings**

- a. Future Meetings and Conference Calls, to be Determined During the Meeting

#### **\*\*\* Participation via Conference Call \*\*\***

Conference call participation in this meeting may be accessed by following these instructions:

- Call this number: (816) 650-0669
- Follow prerecorded instructions
- Enter Access Code: 831018#

## “Balance Resources and Demand” SDT Roster

Raymond Vice (Chairman) Manager Operations Engineering	Southern Company Services, Inc. Bulk Power Operations PCC Corp. HQ P.O. Box 2641 Birmingham, Alabama 35291-8210	205-257-6209 (office) 205-910-0196 (cell) 205-257-6663 (fax) rlvice@southernco.com
Bill Aycock Manager, Market Operations	Transmission Policy Entergy Service Inc. 5201 West Barraque Pine Bluff, AR 71602	870-541-3912 (office) 870-692-2701 (cell) 870-541-3936 (fax) waycock@entergy.com
Stephen J. Beuning Manager, Transmission Operations	Xcel Energy Marketing 512 Nicollet Mall, RS-5 Minneapolis, MN 55401	612-330-7987 (office) 612-581-6785 (cell) stephen.beuning@xemkt.com
Jim Cyrulewski Vice President-Asset Performance & Engineering	International Transmission Co. 39500 Orchard Hill Place, Suite 205 Novi, Michigan 48375	248-374-7130 (office) 248-515-1109 (cell) jcyrulewskij@itctransco.com
Albert DiCaprio (Requestor) Corporate Strategist	PJM Interconnection, L.L.C. 955 Jefferson Avenue Valley Forge Corporate Center Norristown, PA 19403-2497	610-666-8854 (office) 610-666-4282 (fax) <a href="mailto:dicapram@pjm.com">dicapram@pjm.com</a>
Robert L. Dintelman Assistant Executive Director, or LeRoy Patterson Director, Operations & Training	WECC University of Utah, Research Park 615 Arapeen Dirve, Suite 210 Salt Lake City, UT 84108-1262	801-582-0353 ext 104 (office) 801-582-3918 (fax) bob@wecc.biz
Mark R. Henry Manager of Compliance	ERCOT 7620 Metro Center Drive Austin, TX 78744	512-225-7021 (office) 512-225-7020 (fax) mhenry@ercot.com
Doug Hils Manager, Control Area Operations	Cinergy 139 East 4 <sup>th</sup> Street Room 635 – Annex Cincinnati, Ohio 45202	513-287-2149 (office) 513-287-3812 (fax) doug.hils@cinergy.com
Stanley E. Kopman Director, Planning & Compliance	NPCC 1515 Broadway 43 <sup>rd</sup> Floor New York, NY 10036-8901	212-840-8060 (office) 212-302-2782 (fax) skopman@npcc.org
Maureen Long NERC Procedures Manager	NERC Miami, Florida	305-891-5497 (office) <a href="mailto:melong@ieee.org">melong@ieee.org</a> <a href="mailto:maureenlong@earthlink.net">maureenlong@earthlink.net</a>
Carl Monroe Vice President Operations	Southwest Power Pool 415 North McKinley Plaza West -- #700 Little Rock, AR 72205	501-664-0146 (office) 501-664-0146 (fax) cmonroe@spp.org
Thomas J. Vandervort Manager - Resources	NERC Princeton Forrestal Village 116-390 Village Boulevard Princeton, NJ 08540-5731	609-452-8060 (office) 609-452-9550 (fax) tom.vandervort@nerc.net
Lee Xanthakos System Control Manager	South Carolina Electric and Gas MC 204 Columbia, SC 29218	803-217-6058 (office) 803-331-3271 (cell) 803-933-8041 (fax) <a href="mailto:pxanthakos@scana.com">pxanthakos@scana.com</a>
List Server for Standard DT		<a href="mailto:balressdt@nerc.com">balressdt@nerc.com</a>

## Parliamentary Procedures

Based on Robert's Rules of Order, Newly Revised, 10th Edition, plus "Organization and Procedures Manual for the NERC Standing Committees"

### Motions

Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to...	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and can not reverse the intent of the main motion.
Reconsider a Motion already approved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion.
End debate	Call for the Question or End Debate	No	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." Otherwise, this motion is not debatable and subject to 2/3 majority approval.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by 2/3 majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.
Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that can not be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

### Notes on Motions

**Seconds.** A Motion must have a second to ensure that at least two members wish to discuss the issue. The "second" is not recorded in the minutes. Neither are motions that do not receive a second.

**Announcement by the Chair.** The Chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee "owns" the motion, and must deal with it according to parliamentary procedure.

## Voting

Voting Method	When Used	How Recorded in Minutes
Unanimous Consent	When the Chair senses that the Committee is substantially in agreement, and the Motion needed little or no debate. No actual vote is taken.	The minutes show "by unanimous consent."
Vote by Voice	The standard practice.	The minutes show Approved or Not Approved (or Failed).
Vote by Show of Hands (tally)	To record the number of votes on each side when an issue has engendered substantial debate or appears to be divisive. Also used when a Voice Vote is inconclusive. (The Chair should ask for a Vote by Show of Hands when requested by a member).	The minutes show both vote totals, and then Approved or Not Approved (or Failed).
Vote by Roll Call	To record each member's vote. Each member is called upon by the Secretary,, and the member indicates either "Yes," "No," or "Present" if abstaining.	The minutes will include the list of members, how each voted or abstained, and the vote totals. Those members for which a "Yes," "No," or "Present" is not shown are considered absent for the vote.

### Notes on Voting

(Recommendations from DMB, not necessarily Mr. Robert)

**Abstentions.** When a member abstains, he is not voting on the Motion, and his abstention is not counted in determining the results of the vote. The Chair should not ask for a tally of those who abstained.

**Determining the results.** The results of the vote (other than Unanimous Consent) are determined by dividing the votes in favor by the total votes cast. Abstentions are not counted in the vote and shall not be assumed to be on either side.

**"Unanimous Approval."** Can only be determined by a Roll Call vote because the other methods do not determine whether every member attending the meeting was actually present when the vote was taken, or whether there were abstentions.

**Majorities.** Robert's Rules use a simple majority (one more than half) as the default for most motions. NERC uses 2/3 majority for all motions.



# NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

## NERC ANTITRUST COMPLIANCE GUIDELINES

### I. GENERAL

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

### II. PROHIBITED ACTIVITIES

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

Approved by NERC Board of Trustees  
June 14, 2002

### III. ACTIVITIES THAT ARE PERMITTED

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Organization Standards Process Manual
- Transitional Process for Revising Existing NERC Operating Policies and Planning Standards
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

## Operate Within Interconnection Reliability Operating Limits Standard

---

### Definitions

**Bulk Electric System:** A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and high-voltage transmission system (above 35 kV or as approved in a tariff filed with FERC).

**Cascading Outages:** The uncontrolled successive loss of system elements triggered by an incident at any location that results in the loss of 300 MW or more of networked system load for a minimum of 15 minutes.

**Generator Owner:** The entity that owns the generator.

**Instability:** The inability of the transmission system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances.

**Interconnection Reliability Operating Limit:** A system operating limit which, if exceeded, could lead to instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the bulk electric system.

**Interconnection Reliability Operating Limit Event:** An instance of exceeding an Interconnection Reliability Operating Limit for any length of time.

**Interconnection Reliability Operating Limit Event Duration:** The length of time an Interconnection Reliability Operating Limit is exceeded. The duration is measured from the point where the limit is first exceeded and ends when the value drops below the limit and remains below the limit for at least 30 seconds.

**Occurrence Period:** The time period in which performance is measured and evaluated.

**Performance-reset Period:** The time period that the entity being assessed must operate without any violations to reset the level of non-compliance to zero.

**Operational Planning Analysis:** An analysis of the expected system conditions for the next day's operation and up to 12 months ahead. Expected system conditions include things such as load forecast(s), generation output levels, and known system constraints (transmission facility outages, generator outages, equipment limitations, etc.).

**Real-time:** Present time as opposed to future time.

**Real-time Assessment:** An examination of existing and expected system conditions, conducted by collecting and reviewing immediately available data.

**Real-time Data:** Real-time measured values, state estimator values derived from the measured values, or other calculated values derived from the measured values — may include directly monitored data, Inter-utility data exchange (e.g., Interconnection Control Area Communication Protocol or SCADA Data), and manually collected data.

**Real-time Monitoring:** The act of scanning data and drawing conclusions about what the data indicates.



## Operate Within Interconnection Reliability Operating Limits Standard

---

**Reliability Authority Area:** The collection of generation, transmission, and loads within the boundaries of the organization performing the Reliability Authority function. Its boundary coincides with one or more Balancing Authority areas.

**Self-certification:** A process by which an entity does a self-evaluation to determine if it is compliant with the specific requirements for a reliability standard.

**$T_v$ :** The maximum time that an Interconnection Reliability Operating Limit can be exceeded before the risk to the interconnection becomes greater than acceptable.  $T_v$  may not be greater than 30 minutes.

**Transmission Operator:** The entity that operates the transmission facilities and executes switching orders.

**Uncontrolled Separation:** The unplanned break-up of an interconnection, or portion of an interconnection, that is not the result of automatic action by a special protection system or remedial action scheme operating correctly.

**Wide-Area Impact:** The impact of a single incident resulting in the uncontrolled loss of 300 MW or more of networked system load for a minimum of 15 minutes.

## 200 — Operate Within Interconnection Reliability Operating Limits

- 201 Interconnection Reliability Operating Limit Identification
- 202 Monitoring
- 203 Analyses and Assessments
- 204 Actions
- 205 Data Specification and Collection
- 206 Data Provision
- 207 Processes, Procedures, or Plans
- 208 Reliability Authority Directives

1. Purpose: To prevent instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the bulk electric system.
2. Effective Date: This standard will become effective three months after the latter of either the date the NERC Board of Trustees votes to adopt the Determine Facility Ratings, System Operating Limits, and Transfer Capabilities Standard or three months after the date the NERC Board of Trustees votes to adopt this standard.

Initial Compliance with the individual requirements will be phased in as follows:

- 201 — Interconnection Reliability Operating Limit Identification — six months from implementation of Requirement 604.
- 202 — Monitoring — six months from implementation of Requirement 604.
- 203 — Analyses and Assessments — six months from implementation of Requirement 604.
- 204 — Actions — six months from implementation of Requirement 604.
- 205 — Data Specification & Collection — nine months from implementation of Requirement 604.
- 206 — Data Provision — 12 months from implementation of Requirement 604.
- 207 — Processes, Procedures, or Plans — six months from implementation of Requirement 604.
- 208 — Reliability Authority Directives — nine months from implementation of Requirement 604.

3. Applicability: These requirements apply to entities performing various electric system functions, as defined in the Functional Model. NERC is now developing standards and procedures for the identification and certification of such entities. Until that identification and certification is complete, this standard applies to the existing entities (such as control areas, transmission owners and operators, and generator owners) that are currently performing the defined functions.

In this standard, the terms Balancing Authority, Generator Operator, Generator Owner, Interchange Authority, Load-serving Entity, Reliability Authority, Transmission Operator, and

## **Operate Within Interconnection Reliability Operating Limits Standard**

---

Transmission Owner refer to the entities performing these functions as defined in the Functional Model.

**201 — Interconnection Reliability Operating Limits Identification**

**(a) Requirements**

- (1) The Reliability Authority shall identify and document which Facilities (or groups of Facilities) in its Reliability Authority Area are subject to Interconnection Reliability Operating Limits<sup>1</sup>.
  - (i) All Reliability Authorities that share a Facility (or group of Facilities) shall agree on whether that Facility (or group of Facilities) is (are) subject to Interconnection Reliability Operating Limits.
- (2) The Reliability Authority shall identify Interconnection Reliability Operating Limits for its Reliability Authority Area. Each Interconnection Reliability Operating Limit shall have a  $T_v$  that is smaller than or equal to 30 minutes.
- (3) All Reliability Authorities that share a Facility (or group of Facilities) subject to an Interconnection Reliability Operating Limit shall agree upon the process used to determine that Interconnection Reliability Operating Limit and its associated  $T_v$ .

**(b) Measures**

- (1) The Reliability Authority shall have a list of Facilities (or group of Facilities) in its Reliability Authority Area that are subject to Interconnection Reliability Operating Limits.
  - (i) The Reliability Authority shall have evidence it has reviewed and updated its list of Facilities (or groups of Facilities) to reflect changes in its Reliability Authority Area's system topology.
- (2) The Reliability Authority shall be able to identify the current values of the Interconnection Reliability Operating Limits it monitors. Each of these Interconnection Reliability Operating Limits shall have a  $T_v$  that is smaller than or equal to 30 minutes.
  - (i) The Reliability Authorities that share a Facility (or group of Facilities) shall have an agreed upon process for determining if that Facility (or group of Facilities) is subject to an Interconnection Reliability Operating Limit and for determining the value of that Interconnection Reliability Operating Limit and its associated  $T_v$ .
- (3) The Reliability Authority shall be able to demonstrate that its Interconnection Reliability Operating Limit values and their  $T_v$  reflect current system conditions.

**(c) Regional Differences**

None identified.

---

<sup>1</sup> Each Interconnection Reliability Operating Limit is developed by following the requirements in the Determine Facility Ratings, System Operating Limits, and Transfer Capabilities Standard.

**(d) Compliance Monitoring Process**

- (1) The Reliability Authority shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.
- (2) The Performance-reset Period shall be 12 months from the last violation. The Reliability Authority shall keep data on facilities and limits for three calendar years. The Compliance Monitor shall keep audited data for three calendar years.
- (3) The Reliability Authority shall have the following available upon the request of its Compliance Monitor:
  - (i) List of Facilities (or group of Facilities) in its Reliability Authority Area that are subject to Interconnection Reliability Operating Limits. The list shall be contained on paper, displayed through an Energy Management System, or via another data source.
  - (ii) Evidence that the list of Facilities (or group of Facilities) subject to Interconnection Reliability Operating Limits was updated.
  - (ii) An agreed upon process for determining if a shared Facility (or group of Facilities) is subject to an Interconnection Reliability Operating Limit and for determining the value of that Interconnection Reliability Operating Limit and its associated  $T_v$ .
- (4) The Reliability Authority shall demonstrate that it can identify the current values of the Interconnection Reliability Operating Limits it monitors and shall show that each of these Interconnection Reliability Operating Limits shall have a  $T_v$  that is smaller than or equal to 30 minutes.

**(e) Levels of Noncompliance**

- (1) Level One: No process for determining if shared Facilities (or groups of Facilities) are subject to Interconnection Reliability Operating Limits and for determining the value of that Interconnection Reliability Operating Limit and its associated  $T_v$ .
- (2) Level Two: No evidence that a shared Facility (or group of Facilities) has an Interconnection Reliability Operating Limit with a  $T_v$  that has been agreed to by all Reliability Authorities that share the Facility (or group of Facilities).
- (3) Level Three: A level three noncompliance occurs if either of the following conditions are present:
  - (i) One or more Interconnection Reliability Operating Limits had a  $T_v$  that was greater than 30 minutes.
  - (ii) No evidence that the list of Facilities (or groups of Facilities) subject to Interconnection Reliability Operating Limits was updated.
- (4) Level Four: A level four noncompliance occurs if either of the following conditions are present:
  - (i) Could not identify the current values of the Interconnection Reliability Operating Limits for its Reliability Area.
  - (ii) No list of Facilities (or groups of Facilities) subject to Interconnection Reliability Operating Limits exists for the Reliability Authority Area.

**(f) Sanctions**

- (1) Sanctions for noncompliance shall be applied consistent with the NERC Compliance and Enforcement Matrix. In places where financial sanctions are applied for noncompliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.

## 202 — Monitoring

### (a) Requirements

- (1) The Reliability Authority shall perform Real-time Monitoring of system operating parameters to determine if its Reliability Authority Area is operating within its Interconnection Reliability Operating Limits.

### (b) Measures

- (1) The Reliability Authority shall have a list of Facilities (or groups of Facilities) subject to Interconnection Reliability Operating Limits available for its operations personnel's Real-time use.
- (2) The Reliability Authority shall have Interconnection Reliability Operating Limits available for its operations personnel's Real-time use.
- (3) The Reliability Authority shall have Real-time Data available in a form that system operators can compare to the Interconnection Reliability Operating Limits.
- (4) The Reliability Authority shall monitor system operating parameters and compare these against its Interconnection Reliability Operating Limits.

### (c) Regional Differences

None identified.

### (d) Compliance Monitoring Process

- (1) The Reliability Authority shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.
- (2) The Performance-reset Period shall be 12 months from the last violation. The Reliability Authority shall keep data on limits for three calendar years. The Compliance Monitor shall keep audited data for three calendar years.
- (3) The Reliability Authority shall demonstrate the following upon the request of the Compliance Monitor:
  - (i) System operators actively monitoring and comparing Real-time system operating parameters associated with Interconnection Reliability Operating Limits.

### (e) Levels of Noncompliance

- (1) Level One: Not applicable.
- (2) Level Two: List of Facilities (or groups of Facilities) subject to Interconnection Reliability Operating Limits not available to operations personnel for Real-time use.
- (3) Level Three: Not applicable.

## Operate Within Interconnection Reliability Operating Limits Standard

---

- (4) Level Four: A level four noncompliance occurs if any of the following conditions are present:
- (i) Interconnection Reliability Operating Limits not available to operations personnel for Real-time use; or
  - (ii) Real-time Data not available in a form that can be compared to the Interconnection Reliability Operating Limits; or
  - (iii) System operating parameters not monitored and compared against Interconnection Reliability Operating Limits.

### **(f) Sanctions**

- (1) Sanctions for noncompliance shall be applied consistent with the NERC Compliance and Enforcement Matrix. In places where financial sanctions are applied for noncompliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.



## 203 — Analyses and Assessments

### (a) Requirements

- (1) The Reliability Authority shall perform Operational Planning Analyses to assess whether the planned Bulk Electric System operations within its Reliability Authority Area will exceed any of its Interconnection Reliability Operating Limits.
- (2) The Reliability Authority shall perform Real-time Assessments to determine if its Reliability Authority Area is exceeding any Interconnection Reliability Operating Limits or is expected to exceed any Interconnection Reliability Operating Limits.

### (b) Measures

- (1) The Reliability Authority shall identify operating situations or events that impact its Reliability Authority Area's ability to operate without exceeding any Interconnection Reliability Operating Limits.
  - (i) The Reliability Authority shall conduct an Operational Planning Analysis at least once each day, evaluating the next day's projected system operating conditions.
  - (ii) The Reliability Authority shall conduct a Real-time Assessment periodically, but at least once every 30 minutes.

### (c) Regional Differences

None identified.

### (d) Compliance Monitoring Process

- (1) The Reliability Authority shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may also use scheduled on-site reviews once every three years, and investigations upon complaint, to assess performance.
- (2) The Performance-reset Period shall be 12 months from the last violation. The Compliance Monitor shall keep audited data for three calendar years.
- (3) The Reliability Authority shall identify the following upon the request of the Compliance Monitor:
  - (i) The time the most recent Operational Planning Analysis was conducted.
  - (ii) Whether the planned Bulk Electric System operations within the Reliability Authority's Reliability Authority Area will exceed any of its Interconnection Reliability Operating Limits.
  - (iii) The time the most recent Real-time Assessment was conducted.
  - (iv) Whether the Real-time Assessment identified if its Reliability Authority Area is exceeding any Interconnection Reliability Operating Limits or is expected to exceed any Interconnection Reliability Operating Limits.

**(e) Levels of Noncompliance**

- (1) Level One: Not applicable.
- (2) Level Two: Not applicable.
- (3) Level Three: A level three noncompliance exists if any of the following conditions are present:
  - (i) No indication that an Operational Planning Analysis was conducted at least once each day.
  - (ii) No indication that a Real-time Assessment was conducted at least once each 30 minutes.
- (4) Level Four: A level four noncompliance exists if either of the following conditions are present:
  - (i) The Reliability Authority could not identify whether the planned Bulk Electric System operations within its Reliability Authority Area is expected to exceed any of its Interconnection Reliability Operating Limits, based on the results of the most recent Operational Planning Analysis.
  - (ii) The Reliability Authority could not identify whether the most recent Real-time Assessment identified if its Reliability Authority Area is exceeding any Interconnection Reliability Operating Limits or is expected to exceed any Interconnection Reliability Operating Limits.

**(f) Sanctions**

- (1) Sanctions for noncompliance shall be applied consistent with the NERC Compliance and Enforcement Matrix. In places where financial sanctions are applied for noncompliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.

## 204 — Actions

### (a) Requirements

- (1) The Reliability Authority shall, without delay, act<sup>2</sup> or direct others to act to:
  - (i) Prevent instances where Interconnection Reliability Operating Limits may be exceeded.
  - (ii) Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded.
- (2) The Reliability Authority shall include a statement in each Interconnection Reliability Operating Limit-related directive, that informs the recipient that the directive is related to an Interconnection Reliability Operating Limit.
- (3) The Reliability Authority shall document instances of exceeding Interconnection Reliability Operating Limits and shall document and complete an Interconnection Reliability Operating Limit Violation Report for instances of exceeding Interconnection Reliability Operating Limits for time greater than  $T_v$ .

### (b) Measures

- (1) The Reliability Authority shall have documentation to support each instance where actions were taken or directives were issued to mitigate the magnitude and duration of exceeding an Interconnection Reliability Operating Limit.
  - (i) The documentation shall include the actions taken or directives issued, the magnitude of the event, and the duration of the event. (This data may be from an operating log, may be from the entity's energy management system, or may be from some other source.)
  - (i) The duration of the event shall be measured from the point when the limit is exceeded to the point when the system has returned to a state that is within the Interconnection Reliability Operating Limit for a minimum of one minute.
- (2) The Reliability Authority shall report each instance of exceeding an Interconnection Reliability Operating Limit for time greater than  $T_v$ .
  - (i) The Reliability Authority shall complete an Interconnection Reliability Operating Limit Violation Report and shall file the report with its Compliance Monitor within five business days of the initiation of the event. (The report shall include the date and time of the event, identification of which Interconnection Reliability Operating Limit was violated and the  $T_v$  for that limit, magnitude and duration of exceeding the Interconnection Reliability Operating Limit, actions taken or directives issued and

---

<sup>2</sup> Note that the Reliability Authority is expected to act without delay and may choose to take 'no overt action' and this may be an acceptable action as long as it is documented. Taking 'no overt action' is not the same as ignoring the problem.

the time these were initiated or issued, and an explanation of results of actions or directives.)

**(c) Regional Differences**

None identified.

**(d) Compliance Monitoring Process**

- (1) The Reliability Authority shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.
- (2) The Performance-reset Period shall be 12 months from the last violation. The Reliability Authority shall keep Interconnection Reliability Operating Limit Violation Reports, operations logs, or other documentation for three calendar years. The Compliance Monitor shall keep audited data for three calendar years.
- (3) The Reliability Authority shall have the following available upon the request of its Compliance Monitor:
  - (i) Operations logs or other documentation indicating the magnitude and duration of each instance of exceeding an Interconnection Reliability Operating Limit and the actions or directives issued for each of these instances.
  - (ii) Interconnection Reliability Operating Limit Violation Reports.

**(e) Levels of Noncompliance<sup>3</sup>**

- (1) Level One: Interconnection Reliability Operating Limit exceeded for a time less than or equal to  $T_v$  and no documentation to indicate actions taken or directives issued to mitigate the instance.
- (2) Level Two: Not applicable.
- (3) Level Three: Not applicable.
- (4) Level Four: Interconnection Reliability Operating Limit exceeded for time greater than  $T_v$ .

---

<sup>3</sup> Note that the Reliability Authority is expected to act without delay and may choose to take 'no overt action' and this may be an acceptable action as long as it is documented. Taking 'no overt action' is not the same as ignoring the problem.

**Operate Within Interconnection Reliability Operating Limits Standard**

**(f) Sanctions**

(1) Sanctions for noncompliance shall be applied consistent with the NERC Compliance and Enforcement Matrix.

- (i) Level one noncompliance sanctions shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.
- (ii) Level four noncompliance sanctions shall be the greater of the fixed dollar sanctions listed in the matrix, or the dollar amount that corresponds to the magnitude and duration of the event as highlighted in the following table:

If the Maximum Value % over the Limit (measured after the event duration exceeds $T_v$ ) is: <small>Max Value % = (Max Value/IROL limit - 1)*100</small>	And the event duration exceeds its $T_v$ by ___ minutes:	Then Multiply the Level 4 \$ sanction by:
0% < Max Value % ≤ 5%	$T_v < \text{Duration} \leq T_v + 5$ minutes	5
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10$ minutes	10
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15$ minutes	15
	$\text{Duration} > T_v + 15$ minutes	20
5% < Max Value % ≤ 10%	$T_v < \text{Duration} \leq T_v + 5$ minutes	10
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10$ minutes	15
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15$ minutes	20
	$\text{Duration} > T_v + 15$ minutes	25
10% < Max Value % ≤ 15%	$T_v < \text{Duration} \leq T_v + 5$ minutes	15
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10$ minutes	20
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15$ minutes	25
	$\text{Duration} > T_v + 15$ minutes	30
15% < Max Value % ≤ 20%	$T_v < \text{Duration} \leq T_v + 5$ minutes	20
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10$ minutes	25
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15$ minutes	30
	$\text{Duration} > T_v + 15$ minutes	35
20% < Max Value % ≤ 25%	$T_v < \text{Duration} \leq T_v + 5$ minutes	25
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10$ minutes	30
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15$ minutes	35
	$\text{Duration} > T_v + 15$ minutes	40
25% < Max Value % ≤ 30%	$T_v < \text{Duration} \leq T_v + 5$ minutes	30
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10$ minutes	35
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15$ minutes	40
	$\text{Duration} > T_v + 15$ minutes	45

## 205 — Data Specification and Collection

### (a) Requirements

- (1) The Reliability Authority shall specify and collect the data it needs to support Real-time Monitoring, Operational Planning Analyses, and Real-time Assessments conducted relative to operating within its Reliability Authority Area's Interconnection Reliability Operating Limits. The Reliability Authority shall collect this data from the entities performing functions that have Facilities monitored by the Reliability Authority, and from entities that provide Real-time Facility status to the Reliability Authority. This includes specifying and collecting data from the following:
  - (i) Balancing Authorities
  - (ii) Generator Owners
  - (iii) Generator Operators
  - (iv) Load-serving Entities
  - (v) Reliability Authorities
  - (vi) Transmission Operators
  - (vii) Transmission Owners
- (2) The Reliability Authority shall specify when to supply data (based on its hardware and software requirements, and the time needed to do its Operational Planning Analyses).
- (3) The Reliability Authority shall notify its Compliance Monitor when both of the following conditions are present:
  - (i) An entity that has data needed to support Real-time Monitoring, Operational Planning, or Real-time Assessments relative to operating within the Reliability Authority's Reliability Authority Area has not provided data as specified, and
  - (ii) The Reliability Authority was unable to resolve the issue with the entity responsible for providing the data.

### (b) Measures

- (1) The Reliability Authority shall have a documented specification for data needed to build and maintain models needed to support Real-time Monitoring, Operational Planning Analyses, and Real-time Assessments relative to Interconnection Reliability Operating Limits.
  - (i) Specification shall include a list of required data, a mutually agreeable format, and timeframe and periodicity for providing data.
  - (ii) Specification shall address the data provision process to use when automated Real-time system operating data is unavailable.
- (2) The Reliability Authority shall have evidence that it has distributed its data specification to entities that have Facilities monitored by the Reliability

Authority and to entities that provide Facility status to the Reliability Authority.

- (3) The Reliability Authority shall notify its Compliance Monitor when an entity that has Facilities monitored by the Reliability Authority, or an entity that provides Facility status to the Reliability Authority, does not provide data as specified and the Reliability Authority was unable to resolve the issue with the entity responsible for providing the data.
  - (i) If the Reliability Authority does not receive data as specified, and is unable to resolve the situation, then the Reliability Authority shall notify its Compliance Monitor within five business days of discovering that the data is missing.

### **(c) Regional Differences**

None identified.

### **(d) Compliance Monitoring Process**

- (1) The Reliability Authority shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.
- (2) The Performance-reset Period shall be 12 months from the last violation. The Reliability Authority shall keep its data specification(s) for three calendar years. The Compliance Monitor shall keep audited data for three calendar years.
- (3) The Reliability Authority shall have the following available upon the request of the Compliance Monitor:
  - (i) Data specification(s).
  - (ii) Proof of distribution of the data specification(s).

### **(e) Levels of Noncompliance**

- (1) Level One: Data specification incomplete (missing either the list of required data, a mutually agreeable format, a timeframe for providing data, or a data provision process to use when automated real-time system operating data is unavailable).
- (2) Level Two: No data specification or the specification not distributed to the entities that have Facilities monitored by the Reliability Authority and the entities that provide the Reliability Authority with Facility status.
- (3) Level Three: Not applicable.
- (4) Level Four: Not applicable.

**(f) Sanctions**

- (1) Sanctions for noncompliance shall be applied consistent with the NERC Compliance and Enforcement Matrix. In places where sanctions are applied for noncompliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.



## 206 — Data Provision

### (a) Requirements

- (1) Each entity performing one of the following functions shall provide data and real-time Facility status, as specified, to the Reliability Authority(ies) with which it has a reliability relationship. The data is limited to data needed by the Reliability Authority to support Real-time Monitoring, Operational Planning Analyses, and Real-time Assessments conducted relative to operating within its Reliability Authority Area's Interconnection Reliability Operating Limits.
  - (i) Balancing Authorities
  - (ii) Generator Owners
  - (iii) Generator Operators
  - (iv) Load-serving Entities
  - (v) Reliability Authorities
  - (vi) Transmission Operators
  - (vii) Transmission Owners

### (b) Measures

- (1) The responsible entity shall have evidence that it has provided data, as specified, to the requesting Reliability Authority, within the timeframe specified, in the mutually agreed upon format.

### (c) Regional Differences

None identified.

### (d) Compliance Monitoring Process

- (1) The responsible entity shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.
- (2) The Performance-reset Period is 12 months from the last violation. The responsible entity shall keep data transmittal documentation for three calendar years. The Compliance Monitor shall keep audited data for three calendar years.
- (3) The responsible entity shall have the following available upon the request of the Compliance Monitor:
  - (i) Evidence indicating data was sent to the Reliability Authority or evidence that the entity responsible committed to providing the data identified in the specification.

**(e) Levels of Noncompliance**

- (1) Level One: Not applicable.
- (2) Level Two: Not applicable.
- (3) Level Three: Not applicable.
- (4) Level Four: Data was not provided to the Reliability Authority as specified and the situation was not resolved with the Reliability Authority.

**(f) Sanctions**

- (1) Sanctions for noncompliance shall be applied consistent with the NERC Compliance and Enforcement Matrix. In places where sanctions are applied for noncompliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.

**207 — Processes, Procedures, or Plans for Preventing and Mitigating Interconnection Reliability Operating Limits**

**(a) Requirements**

- (1) The Reliability Authority shall have one or more processes, procedures, or plans that identify actions it shall take or actions it shall direct others to take, for both prevention and mitigation of instances of exceeding its Interconnection Reliability Operating Limits.

**(b) Measures**

- (1) The Reliability Authority shall have one or more documented processes, procedures, or plans that address both preventing and mitigating instances of exceeding Interconnection Reliability Operating Limits. The processes, procedures, or plans shall identify and be coordinated with those entities responsible for taking actions and with those entities impacted by such actions.

**(c) Regional Differences**

None identified.

**(d) Compliance Monitoring Process**

- (1) The Reliability Authority shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.
- (2) The Performance-reset Period is 12 months from the last violation. The Reliability Authority shall keep its action plan for three calendar years. The Compliance Monitor shall keep audit records for three calendar years.
- (3) The Reliability Authority shall make the following available for inspection by the Compliance Monitor upon request:
  - (i) Processes, procedures, or plans that address preventing and mitigating instances of exceeding Interconnection Reliability Operating Limits.

**(e) Levels of Noncompliance**

- (1) Level One: Processes, procedures, or plans exist but weren't coordinated with all involved and impacted entities.
- (2) Level Two: Processes, procedures, or plans exist but weren't coordinated with any involved or any impacted entities.
- (3) Level Three: Processes, procedures, or plans exist but do not address both preventing and mitigating instances of exceeding Interconnection Reliability Limits.
- (4) Level Four: No processes, procedures, or plans exist addressing preventing and mitigating instances of exceeding Interconnection Reliability Operating Limits.

**(f) Sanctions**

- (1) Sanctions for noncompliance shall be applied consistent with the NERC Compliance and Enforcement Matrix. In places where sanctions are applied for noncompliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.

## 208 — Reliability Authority Directives

### (a) Requirements

- (1) The Transmission Operator, Balancing Authority, and Interchange Authority shall follow the Reliability Authority's directives to:
  - (i) Prevent instances where Interconnection Reliability Operating Limits may be exceeded.
  - (ii) Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded.
- (2) The responsible entity shall document the Reliability Authority's directives and the actions taken.

### (b) Measures

- (1) The responsible entity shall follow the Reliability Authority's directives and shall document the directives and actions taken to meet the directives.
- (2) The responsible entity shall document via an operations log or other data source, the following for each directive it receives relative to an Interconnection Reliability Operating Limit:
  - (i) Date and time of directive received.
  - (ii) Directive issued.
  - (iii) Actions taken in response to directive.

### (c) Regional Differences

None identified.

### (d) Compliance Monitoring Process

- (1) The responsible entity shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor may also use scheduled on-site reviews every three years, and investigations upon complaint to assess performance.
- (2) The Performance-reset Period is 12 months from the last violation. The responsible entity shall keep its documentation for three calendar years. The Compliance Monitor shall keep audit records for three calendar years.
- (3) The responsible entity shall make the following available for inspection by the Compliance Monitor upon request:
  - (i) Operations log or other data source(s) to show the following for each instance of being issued a Reliability Authority directive relative to an Interconnection Reliability Operating Limit:
    - 1) Date and time of each directive received.
    - 2) Directive issued.
    - 3) Actions taken in response to directive.

**(e) Levels of Noncompliance**

- (1) Level One: The responsible entity followed Reliability Authority's directives relative to preventing or mitigating instances of exceeding Interconnection Reliability Operating Limits but did not document the date and time of each directive received, the directive received, and the actions taken in response to the directive.
- (2) Level Two: Not applicable.
- (3) Level Three: Not applicable.
- (4) Level Four: The responsible entity did not follow the Reliability Authority's directives.

**(f) Sanctions**

- (1) Sanctions for noncompliance shall be applied consistent with the NERC Compliance and Enforcement Matrix. In places where sanctions are applied for noncompliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability  
Operating Limits**

---

**Implementation Plan Contents:**

Prerequisite Approvals ..... 2  
    Applicability During Transition to Functional Model ..... 2

Retirement of Sections of Operating Policies ..... 3

Policy Retirements or Revisions ..... 5

Compliance with Standard ..... 15

Functions that Must Comply With the Requirements ..... 15  
    Phased-in Compliance ..... 16

## **Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

---

### **Prerequisite Approvals**

The Determine Facility Ratings, System Operating Limits and Transfer Capabilities Standard must be implemented before this standard can be implemented.

### **Applicability during Transition to Functional Model**

The requirements in Standard 200 apply to entities performing various electric system functions, as defined in the functional model approved by the NERC Board of Trustees in June 2001. NERC is now developing standards and procedures for the identification and certification of such entities. Until that identification and certification is complete, these standards apply to the existing entities (such as control areas, transmission owners and operators, and generation owners and operators) that are currently performing the defined functions.



## Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits

---

### Retirement of Sections of Operating Policies

Many elements contained in Standard 200 address the same or similar performance objectives as sections of Operating Policy 2, Operating Policy 4, Operating Policy 5 and Operating Policy 9. To eliminate duplication and minimize confusion, the following sections of existing Operating Policies should be retired when this standard is implemented. Justification for these retirements is provided in the tables on the following pages.

#### Operating Policy 2:

- Standard A.1
- Standard A.1.2
- Standard A.2
- Requirement A.1 (just last 2 bullets)
- Requirement A.1.1
- Requirement A.1.2
- Requirement B.5

#### Operating Policy 4:

- Requirement A.1
- Requirement B.3
- Requirement B.3.1
- Requirement B.4
- Requirement B.4.1
- Appendix 4BA

#### Operating Policy 5:

- Requirement 5.C.1
- Requirement 5.C.2

#### Operating Policy 9:

- Requirement A.1
- Requirement A.1.1
- Requirement A.1.2

#### Other Changes:

- Operating Policy 4, Requirement A.2 should be ‘tagged’ to note that the requirement is no longer applicable to system operators working for entities performing the Reliability Authority function, but is still applicable to system operators working for entities performing the Transmission Operator function.



**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

**Policy Retirements or Revisions**

The following tables identify the sections of existing Operating Policies that shall be retired when this standard is implemented.

Policy 2 – Transmission Language in Policy	Standard 200 Replacement Requirement
<p><b>Standard A.1.</b>  <b>Basic reliability requirement regarding single contingencies.</b> All CONTROL AREAS shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.</p>	<p>204. 1.1 The Reliability Authority shall act or direct others to act to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul>
<p><b>Standard A .1 .2.</b>  <b>Operating Security Limits.</b> Operating Security Limits define the acceptable operating boundaries.</p>	<p>201.1 The Reliability Authority shall identify and document which facilities (or groups of facilities) in the Reliability Authority’s reliability area are subject to Interconnection Reliability Operating Limits.</p> <p>201.2 The Reliability Authority shall identify each Interconnection Reliability Operating Limit within the Reliability Authority’s reliability area.</p> <ul style="list-style-type: none"> <li>- The Reliability Authority shall identify a T<sub>v</sub> for each Interconnection Reliability Operating Limit.</li> </ul>
<p><b>Standard A.2.</b>  <b>Return from OPERATING SECURITY LIMIT Violation.</b> Following a contingency or other event that results in an OPERATING SECURITY LIMIT violation, the CONTROL AREA shall return its transmission system to within OPERATING SECURITY LIMITS soon as possible, but no longer than 30 minutes.</p>	<p>204.1.1 The Reliability Authority shall act or direct others to act to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

Policy 2 – Transmission Language in Policy	Standard 200 Replacement
<p><b>Requirement A.1.</b> Policies for dealing with transmission security. CONTROL AREAS, individually and jointly, shall develop, maintain, and implement formal policies and procedures to provide for transmission security. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional security, including:</p> <ul style="list-style-type: none"> <li>- Equipment ratings</li> <li>- Monitoring and controlling voltage levels and real and reactive power flows</li> <li>- Switching transmission elements</li> <li>- Planned outages of transmission elements</li> <li>- <b>Development of Operating Security Limits</b></li> <li>- <b>Responding to OPERATING SECURITY LIMIT violations.</b></li> </ul>	<p><i>(Only highlighted items should be retired.)</i></p> <p>201.1 The Reliability Authority shall identify and document which Facilities (or groups of Facilities) in its Reliability Authority Area are subject to Interconnection Reliability Operating Limits<sup>1</sup>.</p> <p>201.2 The Reliability Authority shall identify Interconnection Reliability Operating Limits for its Reliability Authority Area. Each Interconnection Reliability Operating Limit shall have a T<sub>v</sub> that is smaller than or equal to 30 minutes.</p> <p>201.3 All Reliability Authorities that share a Facility (or group of Facilities) subject to an Interconnection Reliability Operating Limit shall agree upon the process used to determine that Interconnection Reliability Operating Limit and its associated T<sub>v</sub></p> <p>207.1.1 The Reliability Authority shall have one or more processes, procedures or plans that identify actions it shall take or actions it shall direct others to take, for both prevention and mitigation of instances of exceeding its Interconnection Reliability Operating Limits.</p> <p><i>(Operating Security Limits that, when exceeded may cause instability and cascading outages on the bulk electric system have now been defined as Interconnection Reliability Operating Limits (IROLs) within this standard.)</i></p>
<p><b>Requirement A.1.1.</b> Responsibility for transmission security. When OPERATING SECURITY LIMIT violations occur, or are expected to occur, the CONTROL AREAS affected by and the CONTROL AREAS contributing to these violations shall implement established joint actions to restore transmission security.</p>	<p>204.1.1 The Reliability Authority shall, without delay, act or direct others to act to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul>

<sup>1</sup> Each IROL is developed by following the requirements in the Determine Facility Ratings, System Operating Limits and Transfer Capabilities Standard.

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

Policy 2 – Transmission Language in Policy	Standard 200 Replacement
<p><b>Requirement A.1.2.</b> Action to keep transmission within limits. CONTROL AREAS shall take all appropriate action up to and including shedding of firm load in order to comply with Standard 2.A.2.</p>	<p>204.1.1 The Reliability Authority shall, without delay, act or direct others to act to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul> <p>208.1.1 The Transmission Operator, Balancing Authority and Interchange Authority shall follow the Reliability Authority’s directives to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul>
<p><b>Requirement B.5.</b> <b>Preventing Voltage Collapse.</b> The SYSTEM OPERATOR shall take corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.</p>	<p>204.1.1 The Reliability Authority shall act or direct others to act to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul> <p><i>(Note that IROLs may be voltage limits)</i></p>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<p align="center"><b>Policy 4 – System Coordination</b></p> <p align="center"><b>Language in Policy</b></p>	<p align="center"><b>Standard 200 Replacement</b></p>
<p><b>Section A – Monitoring System Conditions</b>  <b>Requirement A.1 Resources.</b> The system operator shall be kept informed of all generation and transmission resources available for use.</p>	<p><i>Keep for transmission operator’s system operators</i></p> <p>205.1.1 The Reliability Authority shall specify and collect the data it needs to support Real-Time Monitoring, Operational Planning Analyses, and Real-Time Assessments conducted relative to operating within its reliability area’s Interconnection Reliability Operating Limits. The Reliability Authority shall collect this data from the entities performing functions that have Facilities monitored by the Reliability Authority, and from entities that provide Real-time Facility status to the Reliability Authority. This includes specifying and collecting data from the following:</p> <ul style="list-style-type: none"> <li>- Balancing Authorities</li> <li>- Generator Owners</li> <li>- Generator Operators</li> <li>- Reliability Authorities</li> <li>- Transmission Operators</li> <li>- Transmission Owners</li> <li>- Load Serving Entities</li> </ul>
<p><b>Requirement A.2 Transmission status and data.</b> System operators shall monitor transmission line status, MW and MVAR flows, voltage, LTC settings and status of rotating and static reactive resources</p>	<p><i>Keep for transmission operator’s system operators</i></p> <p>202.1.1 The Reliability Authority shall perform Real-time Monitoring of system operating parameters to determine if the Reliability Authority Area is operating within its Interconnection Reliability Operating Limits.</p>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<p align="center"><b>Policy 4 – System Coordination</b></p> <p align="center"><b>Language in Policy</b></p>	<p align="center"><b>Standard 200 Replacement</b></p>
<p><b>B3 – Data required from control areas</b></p> <p><b>3. Data required from Control Areas.</b> Each CONTROL AREA shall provide its SECURITY COORDINATOR(S) with the Electric System Security Data that is necessary to allow THE SECURITY COORDINATOR(S) to perform its operational security assessments and coordinate reliable operations.</p> <p><b>3.1 Data.</b> CONTROL AREAS shall provide the types of data as listed in Appendix 4B, “Electric System Security Data, Section A, Electric System Security Data”, unless otherwise agreed to by the CONTROL AREAS and their SECURITY COORDINATOR(S).</p>	<p>206.1.1 Each entity performing one of the following functions shall provide data, as specified, to the Reliability Authority(ies) with which it has a reliability relationship.</p> <ul style="list-style-type: none"> <li>- Balancing Authorities</li> <li>- Generator Owners</li> <li>- Generator Operators</li> <li>- Reliability Authorities</li> <li>- Transmission Operators</li> <li>- Transmission Owners</li> <li>- Load Serving Entities</li> </ul>
<p><b>4. Data exchange among SECURITY COORDINATORS.</b> Upon request, SECURITY COORDINATORS shall, via the ISN, exchange with each other Electric Security Data that is necessary to allow the SECURITY COORDINATORS to perform their operational security assessments and coordinate their reliable operations.</p>	<p>206.1.1 Each entity performing one of the following functions shall provide data, as specified, to the Reliability Authority(ies) with which it has a reliability relationship.</p> <ul style="list-style-type: none"> <li>- Balancing Authorities</li> <li>- Generator Owners</li> <li>- Generator Operators</li> <li>- Reliability Authorities</li> <li>- Transmission Operators</li> <li>- Transmission Owners</li> <li>- Load Serving Entities</li> </ul>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

---

<p align="center"><b>Policy 4 – System Coordination</b></p> <p align="center"><b>Language in Policy</b></p>	<p align="center"><b>Standard 200 Replacement</b></p>
<p><b>4.1. Data.</b> SECURITY COORDINATORS shall share with each other the types of data as listed in Appendix 4B, “Electric System Security Data, Section A, Electric System Security Data”, unless otherwise agreed to.</p>	<p>206.1.1 Each entity performing one of the following functions shall provide data, as specified, to the Reliability Authority(ies) with which it has a reliability relationship.</p> <ul style="list-style-type: none"> <li>- Balancing Authorities</li> <li>- Generator Owners</li> <li>- Generator Operators</li> <li>- Reliability Authorities</li> <li>- Transmission Operators</li> <li>- Transmission Owners</li> <li>- Load Serving Entities</li> </ul>



**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<p><b>Appendix 4BA</b></p>	<p>205.1.1 The Reliability Authority shall specify and collect the data it needs to support Real-Time Monitoring, Operational Planning Analyses And Real-Time Assessments conducted relative to operating within its Reliability Authority Area’s Interconnection Reliability Operating Limits. The Reliability Authority shall collect this data from the entities performing functions that have Facilities monitored by the Reliability Authority, and from entities that provide Real-time Facility status to the Reliability Authority. This includes specifying and collecting data from the following:</p> <ul style="list-style-type: none"> <li>- Balancing Authorities</li> <li>- Generator Owners</li> <li>- Generator Operators</li> <li>- Reliability Authorities</li> <li>- Transmission Operators</li> <li>- Transmission Owners</li> <li>- Load Serving Entities</li> </ul>
----------------------------	---

<p><b>Policy 5 – Emergency Operations Language in Policy</b></p>	<p><b>Standard 200 Replacement</b></p>
<p><b>Requirement 5.C.1. Relieving security limit violations.</b> Each CONTROL AREA experiencing or materially contributing to an OPERATING SECURITY LIMIT violation shall take immediate steps to relieve the condition.</p>	<p>204.1.1 The Reliability Authority shall, without delay, act or direct others to act to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul> <p>208.1.1 The Transmission Operator, Balancing Authority and Interchange Authority shall follow the Reliability Authority’s directives to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> </ul>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

	<ul style="list-style-type: none"> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul>
<p><b>Requirement 5.C.2 Operator authority and responsibility.</b>  SYSTEM OPERATORS having responsibility for the reliability of the transmission system within a CONTROL AREA, pool, etc. shall be given and shall exercise specific authority to alleviate OPERATING SECURITY LIMIT violations. The authority shall enable the SYSTEM OPERATOR to take timely and appropriate actions including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding load, etc.</p>	<p>204.1.1 The Reliability Authority shall, without delay, act or direct others to act to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul> <p>208.1.1 The Transmission Operator, Balancing Authority And Interchange Authority shall follow the Reliability Authority’s directives to:</p> <ul style="list-style-type: none"> <li>- Prevent instances where Interconnection Reliability Operating Limits may be exceeded</li> <li>- Mitigate the magnitude and duration of instances where Interconnection Reliability Operating Limits have been exceeded</li> </ul>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<p align="center"><b>Policy 9 – Security Coordinator Language in Policy</b></p>	<p align="center"><b>Standard 200 Replacement</b></p>
<p><b>Requirement A.1.</b> <b>Perform security analysis.</b> The RELIABILITY COORDINATORS shall ensure that next-day reliability analyses are performed simultaneously for all CONTROL AREAS and TRANSMISSION PROVIDERS in its RELIABILITY AREA to ensure that the bulk power system can be operated in anticipated normal and contingency conditions.</p>	<p>203.1.1 The Reliability Authority shall perform Operational Planning Analyses to assess whether the planned bulk electric system operations within its Reliability Authority Area will exceed any of its Interconnection Reliability Operating Limits.</p> <p>203.1.2 The Reliability Authority shall perform Real-Time Assessments to determine if its Reliability Authority Area is exceeding any Interconnection Reliability Operating Limits or is expected to exceed any Interconnection Reliability Operating Limits.</p>
<p><b>1.1. Information sharing.</b> Each CONTROL AREA in the SECURITY AREA shall provide information required for system studies, such as critical facility status, load, generation, operating reserve projections, and known INTERCHANGE TRANSACTIONS. This information shall be available by 1200 Central Standard Time for the Eastern Interconnection, and 1200 Pacific Standard Time for the Western Interconnection.</p>	<p>206.1.1 Each entity performing one of the following functions shall provide data, as specified, to the Reliability Authority(ies) with which it has a reliability relationship.</p> <ul style="list-style-type: none"> <li>- Balancing Authority</li> <li>- Generator Owners</li> <li>- Generator Operators</li> <li>- Reliability Authorities</li> <li>- Transmission Operators</li> <li>- Transmission Owners</li> <li>- Load Serving Entities</li> </ul> <p><i>(Note that this data is only a subset of the data addressed in Policy 9 Requirement A.1.1.1)</i></p>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

---

<p><b>Requirement A.1.2.</b> <b>System Studies.</b> The RELIABILITY COORDINATORS shall conduct studies to identify potential interface and other OPERATING RELIABILITY LIMIT violations, including overloaded transmission lines and transformers, voltage and stability limits, etc.</p>	<p>203.1.1 The Reliability Authority shall perform Operational Planning Analyses to assess whether the planned bulk electric system operations within its Reliability Authority Area will exceed any of its Interconnection Reliability Operating Limits.</p> <p>203.1.2 The Reliability Authority shall Perform Real-Time Assessments to determine if its Reliability Authority Area is exceeding any Interconnection Reliability Operating Limits or is expected to exceed any Interconnection Reliability Operating Limits.</p>
---	--

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

---

**Compliance with Standard**

Requirement	Functions that Must Comply With the Requirements							
	Reliability Authority	Balancing Authority	Interchange Authority	Transmission Operator	Transmission Owner	Generator Owner	Generator Operator	Load Serving Entity
201 IROL Identification	X							
202 Monitoring	X							
203 Analyses & Assessments	X							
204 Actions	X							
205 Data Specification & Collection	X							
206 Data Provision	X	X		X	X	X	X	X
207 Processes, Procedures or Plans	X							
208 RA Directives		X	X	X				

## Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits

---

### *Phased-in Compliance*

The following table identifies the implementation date and the earliest compliance date for each requirement.

The implementation date is the date entities are expected to begin meeting the performance identified in this standard. Because this standard rests upon the communication of system operating limits as defined in Requirement 204 - 604 Communication of System Operating Limits, the compliance dates are fixed from that date. Additional time (preparation time) has been added to give entities time needed to fully comply with the requirements. The justification for the staggered effective dates is in the tables on the following pages.

<b>Requirement</b>	<b>Effective Date</b>	<b>Compliance Date</b>
201 - IROL Identification	3 months from BOT adoption	6 months from implementation of Requirement 604
202 – Monitoring	3 months from BOT adoption	6 months from implementation of Requirement 604
203 - Analyses and Assessments	3 months from BOT adoption	6 months from implementation of Requirement 604
204 - Actions	3 months from BOT adoption	6 months from implementation of Requirement 604
205 – Data Specification & Collection	3 months from BOT adoption	9 months from implementation of Requirement 604
206 – Data Provision	3 months from BOT adoption	12 months from implementation of Requirement 604
207 – Processes, Procedures or Plans	3 months from BOT adoption	6 months from implementation of Requirement 604
208 – Reliability Authority Directives	3 months from BOT adoption	9 months from implementation of Requirement 604

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<b>Requirement 201 – IROL Identification</b>		
<b>Measure</b>	<b>Description</b>	<b>Preparation</b>
201.1	<p>The Reliability Authority shall have a list of Facilities (or group of Facilities) in its Reliability Authority Area that are subject to Interconnection Reliability Operating Limits.</p> <p>(i) The Reliability Authority shall have evidence it has reviewed and updated its list of Facilities (or groups of Facilities) to reflect changes in its Reliability Authority Area’s system topology.</p>	<p>This should already be done in some format to comply with current field testing of IRLs and to comply with existing Operating Policy – only additional time needed would be to produce some evidence that list has been updated</p>
201.2	<p>The Reliability Authority shall be able to identify the current values of the Interconnection Reliability Operating Limits it monitors. Each of these Interconnection Reliability Operating Limits shall have a <math>T_v</math> that is smaller than or equal to 30 minutes.</p> <p>(i) The Reliability Authorities that share a Facility (or group of Facilities) shall have an agreed upon process for determining if that Facility (or group of Facilities) is subject to an Interconnection Reliability Operating Limit and for determining the value of that Interconnection Reliability Operating Limit and its associated <math>T_v</math>.</p>	<p>Current policy has a 30-minute response time for all limits. Entities may need additional time to establish variable <math>T_v</math>s for IROLs. This should be done within 6 months.</p> <p>This should already be done in some format to comply with current field testing of IRLs and to comply with existing Operating Policy – only additional time needed would be to put produce some evidence that list has been updated and this could be done in less than a week if needed.</p>
201.3	<p>The Reliability Authority shall be able to demonstrate that its Interconnection Reliability Operating Limit values and their <math>T_v</math> reflect current system conditions.</p>	<p>This should not require any additional work – if limits are being updated to reflect ‘current’ conditions today, then the ability exists.</p>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<b>Requirement 202 – Monitoring</b>		
<b>Measure</b>	<b>Description</b>	<b>Preparation</b>
202.1	The Reliability Authority shall have a list of Facilities (or groups of Facilities) subject to IROLs available for its operations personnel’s Real-time use.	This should already be done in some format to comply with current field testing of IRLs and to comply with existing Operating Policy – only additional time needed would be to produce some evidence that list has been updated
202.2.	The Reliability Authority shall have Interconnection Reliability Operating Limits available for its operations personnel’s Real-time use.	This should already be done in some format to comply with existing Operating Policy – only additional time needed would be to re-title the limits as IROLs.
202.3	The Reliability Authority shall have Real-time Data available in a form that system operators can compare to the Interconnection Reliability Operating Limits.	This should already be done in some format to comply with existing Operating Policy – only additional time needed would be to let system operators know that the limits are called IROLs and may have unique T <sub>v</sub> s.
202..4	The Reliability Authority shall monitor real-time system operating parameters and compare these against its Interconnection Reliability Operating Limits.	This should already be done in some format to comply with existing Operating Policy – only additional time needed would be to let system operators know that the limits are called IROLs and may have unique T <sub>v</sub> s.



**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<b>Requirement 203 – Analyses and Assessments</b>		
<b>Measure</b>	<b>Description</b>	<b>Preparation</b>
203..1	The Reliability Authority shall identify operating situations or events that impact its Reliability Authority Area’s ability to operate without exceeding any Interconnection Reliability Operating Limits.	This should already be done in some format to comply with existing Operating Policy – only additional time needed would be to let system operations personnel know that the limits are called IROLs and may have unique T <sub>v</sub> s.
203.1.i.	The Reliability Authority shall conduct an Operational Planning Analysis at least once each day, evaluating the next day’s projected system operating conditions.	This should already be done to comply with existing Operating Policy – current operating practice in many locations is to do the analysis each day for the day ahead only on weekdays, and to do the ‘weekend ahead’ on Friday. Many entities do not conduct an operational planning analysis on Saturday or Sunday for Sunday and Monday. Entities may need some time to train additional personnel so that the analysis could be conducted every day of the week.
203.1ii	The Reliability Authority shall conduct a Real-time Assessment periodically, but at least once every 30 minutes.	This should already be done to comply with existing Operating Policy – only additional time needed would be to let system operators know that the limits are called IROLs and may have unique T <sub>v</sub> s and to identify that the assessment must be conducted at least once every 30 minutes.

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<b>Requirement 204 - Actions</b>		
<b>Measure</b>	<b>Description</b>	<b>Preparation</b>
204.1.1	<p>The Reliability Authority shall have documentation to support each instance where actions were taken or directives were issued to mitigate the magnitude and duration of exceeding an Interconnection Reliability Operating Limit.</p> <p>(i) The documentation shall include the actions taken or directives issued, the magnitude of the event, and the duration of the event. (This data may be from an operating log, may be from the entity’s energy management system, or may be from some other source.)</p>	<p>This requires that the system operators know which of their limits are IROLs. The actions are done today to comply with Operating Policy.</p>
204.2.	<p>The Reliability Authority shall report each instance of exceeding an Interconnection Reliability Operating Limit for time greater than <math>T_v</math>:</p> <p>(i) The Reliability Authority shall complete an Interconnection Reliability Operating Limit Violation Report and shall file the report with its Compliance Monitor within five business days of the initiation of the event. (The report includes the date and time of the event; identification of which Interconnection Reliability Operating Limit was violated and the <math>T_v</math> for that limit; magnitude and duration of exceeding the Interconnection Reliability Operating Limit after exceeding <math>T_v</math>; actions taken or directives issued and the time these were initiated or issued; explanation of results of actions or directives.)</p>	<p>This requires that the system operators know which of their limits are IROLs. The actions are done today to comply with Operating Policy.</p> <p>This also requires that the Compliance Enforcement Program accept the IROL Violation Report developed by the IROL SDT. The report collects only the information identified in the measure.</p> <p>This also requires that the RA know which entity is acting as its compliance monitor.</p> <p>This also requires that the IROL Violation Report be made available to the RAs.</p>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<b>Requirement 205 – Data Specification &amp; Collection</b>		
<b>Measure</b>	<b>Description</b>	<b>Preparation</b>
205..1	<p>The Reliability Authority shall have a documented specification for data needed to build and maintain models needed to support real time monitoring, operational planning analyses and real time assessments relative to Interconnection Reliability Operating Limits.</p> <p>(i) Specification shall include a list of required data, a mutually agreeable format, and timeframe and periodicity for providing data.</p>	<p>Many entities may not have a data specification in place. The data specification may be distributed in several other documents, and entities may need time to assemble this. Since the data needed is known, even if it is not formally documented, it should be possible to accomplish this documentation within 9 months – this includes time to come to ‘mutual agreement’ with other entities.</p>
205.1.ii	<p>Specification shall address the data provision process to use when automated real-time system operating data is unavailable.</p>	<p>This may not exist and may need to be developed. It should be possible to develop this within the 9 month period identified for developing the complete data specification.</p>
205.2	<p>The Reliability Authority shall have evidence that it has distributed its data specification to the entities that have Facilities monitored by the Reliability Authority and to entities that provide Real-time Facility status to the Reliability Authority.</p>	<p>This requires documentation that wouldn’t be available until after the data specification were completed. This should be done no later than 10 months after the standard is approved – this allows 9 months to develop the specification, and then a month to deliver it.</p>
205..3	<p>The Reliability Authority shall notify its Compliance Monitor when an entity that has Facilities monitored by the Reliability Authority, or an entity that provides Real-time Facility status to the Reliability Authority, does not provide data as specified and the Reliability Authority was unable to resolve the issue with the entity responsible for providing the data .</p>	<p>This requires that the data specification be developed and distributed. This should come into affect a year after the standard is approved. This allows entities some time to ‘field test’ their data specification before compliance is a factor.</p>
205..3.i	<p>If the Reliability Authority does not receive data as specified and is unable to resolve the situation, then the Reliability Authority shall notify its Compliance Monitor within five business days of discovering that the data is missing.</p>	<p>This also requires that the RA know which entity is acting as its compliance monitor.</p>

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

<b>Requirement 206 – Data Provision</b>		
<b>Measure</b>	<b>Description</b>	<b>Preparation</b>
206.2.1	The entity responsible shall have evidence that it has provided data, as specified, to the requesting Reliability Authority, within the time frame specified, in the mutually agreed upon format.	The Data Specification in requirement 205 needs to be in place before this can be implemented. There should be a 12 month delay in implementing compliance with this measure. This allows entities time to work with their RA to come to agreement with a ‘mutually acceptable format’ and gives the entities that must provide the RA with data a 3 month trial and error period for providing data before there is any compliance measurement.

<b>Requirement 207 – Processes, Procedures or Plans</b>		
<b>Measure</b>	<b>Description</b>	<b>Preparation</b>
207.2.1	The Reliability Authority shall have one or more documented processes, procedures, or plans that identify both preventing and mitigating instances of exceeding Interconnection Reliability Operating Limits. The processes, procedures, or plans shall identify and be coordinated with those entities responsible for taking actions and with those entities impacted by such actions.	Entities should have this plan in place now. A six-month delay in compliance should allow everyone time to develop a plan if it doesn’t already exist.

**Implementation Plan for Standard 200 – Operate Within Interconnection Reliability Operating Limits**

---

<b>Requirement 208 – Reliability Authority Directives</b>		
<b>Measure</b>	<b>Description</b>	<b>Preparation</b>
208.2.1	<p>The responsible entity shall follow the Reliability Authority’s directives and shall document the directives and actions taken to meet the directives.</p> <p>The responsible entity shall document via an operations log or other data source, the following for each directive it receives relative to an Interconnection Reliability Operating Limit:</p> <ul style="list-style-type: none"><li>- Date and time of directive received</li><li>- Directive issued</li><li>- Actions taken in response to directive</li></ul>	<p>This should already be done and no additional time for preparation should be needed.</p>

## Questions & Answers About the Operate within Operate within IROLs Standard

---

### Index:

Introduction to Standard .....	3
Expansion on Definitions .....	5
Questions and Answers.....	9
Who needs to comply with this standard? .....	9
When does compliance with this standard start? .....	10
For a System Operator - how does this new standard differ from Operating Policy 2 - Transmission? .....	10
What is an IROL? .....	12
What is the IROL's $T_v$ ? .....	12
Why don't all IROL's have the same $T_v$ ? .....	12
If an RA installs a special protection scheme to reduce the probability of exceeding an IROL for time greater than the limit's $T_v$ , does this eliminate the IROL? .....	12
How do you develop a list of IROL's? .....	12
How do you establish a $T_v$ for an IROL? .....	13
Which instances of exceeding an IROL need to be documented? .....	13
Does the standard require that exceeding an IROL be documented on the system operator's daily log? .....	13
When you exceed an IROL, what do you have to document? .....	13
How many IROLs do you expect the 'typical' RA to have in a year? .....	13
Which instances of exceeding an IROL need to be reported? .....	14
When you exceed an IROL for a time greater than the IROL's $T_v$ , what do you have to report? .....	14
How do you calculate the duration of an IROL event? .....	15
If you exceed an IROL for time greater than $T_v$ , how big is the sanction? .....	16
What is the philosophy behind the sanction for exceeding an IROL for time greater than $T_v$ ? ...	18
Why isn't the sanction linked to the highest value over the course of the event? .....	18
What's the origin of the concept of these sanctions for exceeding IROLs? .....	18
What are you expecting in the requirement for Processes, Procedures or Plans? .....	18
IROL Violation Report .....	19



### Introduction to Standard

This standard requires adherence to the subset of system operating limits<sup>1</sup> identified to prevent instability, uncontrolled separation or cascading outages that adversely impact the reliability of the bulk transmission system. These limits are called interconnection reliability operating limits and are under the authority of the entity performing the reliability authority function. (Note that there are many other system operating limits that are used by system operators working for entities performing the Reliability Authority function and for entities performing the Transmission Operator function. This standard only addresses Interconnection Reliability Operating Limits.)

This standard is aimed at preventing instances of exceeding IROLs – and for those rare occasions when an IROL may be exceeded, the standard is aimed at minimizing the impact of such an event.

The standard is subdivided into eight requirements. Each of the requirements addresses some aspect of monitoring or controlling the transmission system to operate within IROLs. Some of these requirements address underlying responsibilities that must be accomplished as a prerequisite to monitoring and controlling the transmission system relative to IROLs.

201 Interconnection Reliability Operating Limit Identification – requires identification of the facilities that are subject to IROLs, and requires RAs to be able to identify current IROLs. Each IROL must have a  $T_v$  and the  $T_v$  may not be greater than 30 minutes. The list of facilities subject to IROLs must be updated to reflect changes in topology and system conditions. Entities that share a facility must have an agreed upon process for determining whether that facility is subject to an IROL and for developing the IROL and its  $T_v$ . (The entity performing the Reliability Authority Function is responsible for this requirement.)

202 Monitoring – requires monitoring real time data and comparing the data to IROLs to determine if the RA Area is operating within its IROLs (The entity performing the Reliability Authority Function is responsible for this requirement.)

203 Analyses and Assessments – requires that an operational planning analyses be conducted at least once each day to look at the ‘day ahead’ and requires that real-time assessments be conducted at least once every 30 minutes. These analyses and assessments are done to see if the transmission system is expected to be operated within its IROLs and to see if the transmission system is operating within its IROLs. (The entity performing the Reliability Authority Function is responsible for this requirement.)

204 Actions – requires that actions be taken or directives issued to prevent or mitigate instances of exceeding IROLs. These actions and directives must be documented when an IROL is exceeded, and when an IROL is exceeded for a time greater than the IROL’s  $T_v$ , this event must be reported to the Compliance Monitor. The entity that issues a directive relative to an IROL must include a statement in the directive to clarify that the directive is related to an IROL. (The entity performing the Reliability Authority Function is responsible for this requirement.)

205 Data Specification & Collection – requires that a data specification be developed that identifies the data needed for monitoring real-time parameters against IROLs, and for conducting operational planning analyses and real-time assessments relative to operating within its reliability area’s IROLs. The Data Specification must be distributed to entities that are expected to provide data and needs to address what data to provide, a mutually agreeable format for the data, a timeframe and periodicity for providing data, and must address the data provision process to use when automated real-time system operating data is unavailable. The Reliability Authority must notify its Compliance

---

<sup>1</sup> System Operating Limits are established through the standard, “Determine Facility Ratings, Operating Limits and Transfer Capabilities”



## **Questions & Answers About the Operate within Operate within IROLs Standard**

---

Monitor if data is not provided as specified. (The entity performing the Reliability Authority Function is responsible for this requirement.)

206 Data Provision – requires that entities provide the Reliability Authority with data needed to monitor real-time parameters against IROLs, and to conduct operational planning analyses and real-time assessments relative to operating within its reliability area's IROLs. (The entities performing the following Functions are responsible for this requirement: Balancing Authorities, Generator Operators, Generator Owners, Load-serving Entities, Reliability Authorities, Transmission Operators, and Transmission Owners)

207 Processes, Procedures or Plans – requires that there be one or more processes, procedures or plans to address actions to take or directions to issue to prevent and mitigate instances of exceeding IROLs. The processes, procedures or plans must identify and be coordinated with all entities that have to take actions as part of the plan, and with entities that would be impacted by the actions taken in the plan. (The entity performing the Reliability Authority Function is responsible for this requirement.)

208 Reliability Authority Directives – requires that entities follow the Reliability Authority's directives issued to prevent or mitigate instances of exceeding IROLs. The directives issued and the actions taken in response to those directives must be documented. (The entities performing the following functions are responsible for this requirement: Balancing Authority, Interchange Authority, and Transmission Operator.)

### Expansion on Definitions

**Balancing Authority:** Integrates resource plans ahead of time, and maintains load-interchange-generation balance within its metered boundary and supports system frequency in real time.

*(Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.)*

**Bulk Electric System:** A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and high voltage transmission system (above 35 kV or as approved in a tariff filed with FERC).

*(Note – the original definition of this term was ‘circular’ and did not reference any voltage class. The definition was changed to include the reference to a measurable voltage class.)*

**Cascading Outages:** The uncontrolled successive loss of system elements triggered by an incident at any location that results in the loss of 300 MW or more of networked system load for a minimum of 15 minutes.

*(Note –this definition was developed to help provide some measurable basis for determining if a system operating limit is an Interconnection Reliability Operating Limit.)*

**Generator Operator:** Operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.

*Note – This is the definition proposed by the Functional Model Review Task Group for inclusion in the second version of the Functional Model.*

**Generator Owner:** The entity that owns the generator.

*Note – This is the definition proposed by the Functional Model Review Task Group for inclusion in the second version of the Functional Model.*

**Instability:** The inability of the transmission system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances.

**Interconnection Reliability Operating Limit:** A system operating limit which, if exceeded, could lead to instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the bulk electric system.

*(Note – this term was adapted from the term, Interconnection Reliability Limit, drafted by the Operating Limit Definition Task Force.)*

**Interconnection Reliability Operating Limit Event:** An instance of exceeding an interconnection reliability operating limit for any length of time.

*(Note – all IROL Events must be documented.)*

**Interconnection Reliability Operating Limit Event Duration:** The length of time an interconnection reliability operating limit is exceeded. The duration is measured from the point where the limit is first exceeded and ends when the value drops below the limit and remains below the limit for at least 30 seconds.

*(Note –graphics in next section of this Technical Reference shows the application of this 30-second rule.)*

## Questions & Answers About the Operate within Operate within IROLs Standard

---

**Load-serving Entity:** Secures energy and transmission (and related generation services) to serve the end user.

*(Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.)*

**Occurrence period:** The time period in which performance is measured and evaluated.

*(Note – this is a term used by the Compliance Monitors. When you look at the Sanctions Tables, note that the first table’s column headings reference the number of infractions within the Performance-reset period. As the number of infractions within a performance reset period increases, so does the severity of the sanctions.)*

**Operating Procedure** – A document that identifies specific steps or tasks that must be taken by one or more specific operating positions to achieve a single specific operating goal. The steps in an Operating Procedure must be followed in the order in which they are presented, and must be performed by the position(s) identified. A document that lists the specific steps to take in removing a specific transmission line from service is an example of an Operating Procedure.

*(Note – this is a term defined within the Coordinate Operations standard.)*

**Operating Process** – A document that identifies general steps for achieving a generic operating goal. An Operating Process includes steps with options that may be selected depending upon real-time conditions. A guideline for controlling high voltage is an example of an Operating Process.

*(Note – this is a term defined within the Coordinate Operations standard.)*

**Operating Plan-** A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.

*(Note – this is a term defined within the Coordinate Operations standard.)*

### **Operational Planning Analysis:**

An analysis of the expected system conditions for the next day’s operation and up to 12 months ahead. Expected system conditions include things such as load forecast(s), generation output levels, and known system constraints (transmission facility outages, generator outages, equipment limitations, etc.)

*(Note – this standard requires that an operational planning analysis be conducted at least once each day, looking at the day ahead. This does not mean that operational planning analyses are limited to being conducted on a day-ahead basis. For example an operational planning analysis should be conducted as part of approving a transmission line outage – and this operational planning analysis may be conducted several months ahead of the day being reviewed.)*

**Performance-reset Period:** The time period that the entity being assessed must operate without any violations to reset the level of non-compliance to zero.

*(Note – this is a term used by the Compliance Monitors. When you look at the Sanctions Tables, note that the first table’s column headings reference the number of infractions within the Performance-reset period. As the number of infractions within a performance reset period increases, so does the severity of the sanctions.)*

## Questions & Answers About the Operate within Operate within IROLs Standard

---

**Real-time:** Present time as opposed to future time.

**Real-time Assessment:** An examination of existing and expected system conditions, conducted by collecting and reviewing immediately available data.

**Real-time Data:** Real-time measured values, state estimator values derived from the measured values, or other calculated values derived from the measured values – may include directly monitored data, Inter-utility data exchange (e.g., Interconnection Control Area Communication Protocol or SCADA Data), and manually collected data.

**Real-time Monitoring:** The act of scanning data and drawing conclusions about what the data indicates.

*(Note – this definition supports the concept that monitoring is an ‘active’ task. The system operator assigned to monitor system conditions should be prepared to answer questions about what he/she has been monitoring without any preparation time. Simple questions can be used to determine whether or not monitoring has taken place. For example, a system operator who has been monitoring real time data to see if the area under the operator’s direction is approaching or exceeding any IROLs should be able to answer the question, “ Are there any IROLs on your system that have been exceeded? If any have been exceeded, are you approaching or exceeding the IROL’s  $T_v$ ?”*

**Reliability Authority:** Ensures the reliability of the bulk power transmission system within its Reliability Authority Area.

*(Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.)*

**Reliability Authority Area:** The collection of generation, transmission, and loads within the boundaries of the Reliability Authority. Its boundary coincides with one or more Balancing Areas.

*Note – This is the definition proposed by the Functional Model Review Task Group for inclusion in the second version of the Functional Model.*

**Self-certification:** A process by which an entity does a self-evaluation to determine if it is compliant with the specific requirements for a reliability standard.

*Note: This is a term used by the Compliance Monitors.*

**$T_v$ :** The maximum time that an Interconnection Reliability Operating Limit can be exceeded before the risk to the interconnection becomes greater than acceptable.  $T_v$  may not be greater than 30 minutes.

*Note – Operating Policy 2 – Standard A.2 included the following requirement:*

*Following a contingency or other event that results in an OPERATING SECURITY LIMIT violation, the CONTROL AREA shall return its transmission system to within OPERATING SECURITY LIMITS soon as possible, but no longer than 30 minutes.*

*This new standard requires results within ‘ $T_v$ ’ minutes. Some IROLs are so critical that exceeding them for 30 minutes may be too long. See the charts in the next section for examples of how  $T_v$  is used to determine whether an instance of exceeding an IROL must be reported to the Compliance Monitor.*

## **Questions & Answers About the Operate within Operate within IROLs Standard**

---

**Transmission Operator:** The entity that operates the transmission facilities and executes switching orders.

*(Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.)*

**Transmission Owner:** Owns transmission facilities

*(Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.)*

**Uncontrolled Separation:** The unplanned break-up of an interconnection, or portion of an interconnection, that is not the result of automatic action by a special protection system or remedial action scheme operating correctly.

**Wide Area Impact:** The impact of a single incident resulting in the uncontrolled loss of 300 MW or more of networked transmission load for a minimum of 15 minutes.

*(Note – this term was modified to provide a more measurable basis for determining whether a System Operating Limit should also be an Interconnection Reliability Operating Limit. The Standard Drafting Team adopted the threshold criteria used for reporting major incidents to the Department of Energy as the threshold for determining whether an event had a ‘wide area’ impact.)*

## Questions & Answers About the Operate within Operate within IROLs Standard

### Questions and Answers

#### *Who needs to comply with this standard?*

Each of the requirements in the standard assigns responsibility for that requirement to one or more ‘functions.’ The entities performing the listed functions are the entities that must comply with that requirement. Most of the requirements are applicable to entities that perform the Reliability Authority Function – but several functions are assigned responsibility for the Data Provision and RA Directives requirements.

Requirement	Entities that Perform these Functions Must Comply With the Requirements							
	Reliability Authority	Balancing Authority	Interchange Authority	Trans. Operator	Trans. Owner	Gen. Owner	Gen. Operator	Load Serving Entity
201 IROL Identification	X							
202 Monitoring	X							
203 Analyses & Assessments	X							
204 Actions	X							
205 Data Specification & Collection	X							
206 Data Provision	X	X		X	X	X	X	X
207 Processes, Procedures or Plans	X							
208 RA Directives		X	X	X				

### ***When does compliance with this standard start?***

Several things must be in place before entities are expected to come into full compliance with all of the requirements in this standard. Most importantly, the Operate within IROLs Standard can't be implemented until after the Determine Facility Ratings, System Operating Limits and Transfer Capabilities standard has been implemented. The methodology for developing system operating limits must be in place and the RA must identify system operating limits before the RA can be held accountable for identifying which of its system operating limits are IROLs. There are other parts of the standard that will take some time to put into place if they aren't already in place. Some entities performing the RA function may have a detailed data specification that could be used to meet the Data Specification requirement in this standard – but other entities may have handled this requirement on a more casual basis and may need some time to formalize their data specifications.

### ***For a System Operator - how does this new standard differ from Operating Policy 2 - Transmission?***

There are three significant differences between what is expected of system operators under Policy 2, and what is expected of system operators under Standard 200.

#### **Major Difference #1 – Term, 'OSLs' replaced with term, 'IROLs'**

The first difference is a terminology change. The NERC Director–Compliance reports on compliance violations at each NERC Board of Trustees Meeting. He noted an increase in the number of OSL violations, and was directed by the BOT to investigate the cause. The investigation results showed a widespread misunderstanding on what was/was not an OSL. The task force that worked on this problem, called the Operating Limits Definitions Task Force (OLDTF) recommended that the term, "Operating Security Limit" not be used in the future because of the widespread misunderstanding associated with this term. The new standard uses the term, 'Interconnection Reliability Operating Limit – IROL'.

From the Terms Used in the Operating Policies, here is the definition of an Operating Security Limit (OSL):

- The value of a system operating parameter (e.g. total power transfer across an interface) that satisfies the most limiting of prescribed pre- and post-contingency operating criteria as determined by equipment loading capability and acceptable stability and voltage conditions.

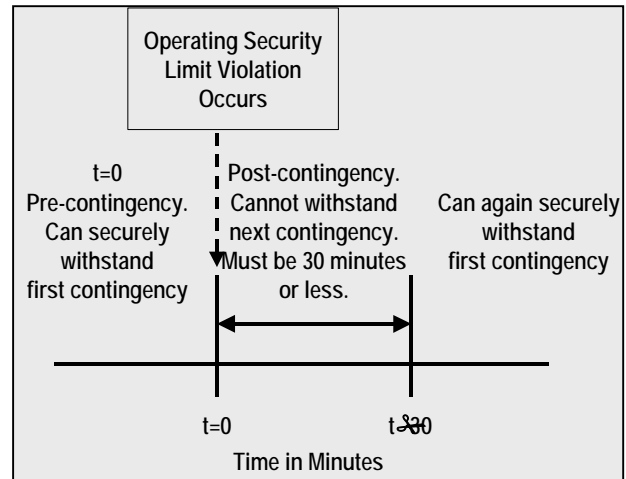
From the Operate within IROLs Standard, here is the definition of an Interconnection Reliability Operating Limit (IROL):

- A system operating limit which, if exceeded, could lead to instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the bulk electric system.

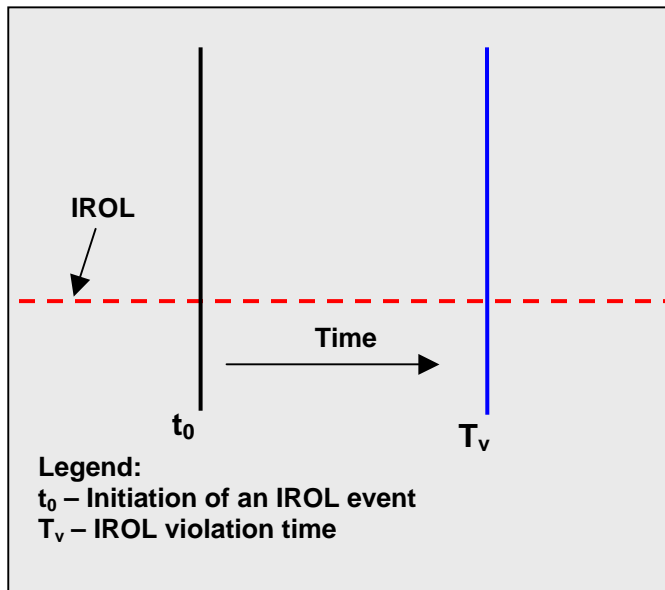
**Major Difference #2 –Resolution time changed from a uniform ‘30-minutes’ for all OSLs to a ‘unique’  $T_v$  that can’t exceed 30 minutes for each IROL**

Policy 2 has a standard ‘30 minute’ response time for resolving any instance of exceeding an operating security limit. The 30 minutes was established to give system operators enough time to recognize the problem and take corrective actions. The new Operate within IROLs standard is designed from a perspective of system risk, and doesn’t have a standard ‘30 minute’ response time.

$T_v$  is the maximum amount of time the system operator has to return to a state that is at or below the limit before being subjected to compliance sanctions.  $T_v$  is based on system risk – and recognizes that some IROLs shouldn’t be exceeded for longer than 10 minutes without causing an unacceptable risk to the interconnection. Each IROL may have its own  $T_v$  but no  $T_v$  may exceed 30 minutes.



*From Policy 2 – all OSLs addressed with the same 30-minute maximum resolution time*



← *Operate within IROLs Standard - each IROL may have its own  $T_v$ .*

*For IROLs that should never be exceeded,  $T_v$  may be zero minutes.*

**Major Difference #3 – New Report for IROL Violations**

Policy 2 requires that a NERC Preliminary Disturbance Report be completed for OSL Violations that exceed 30 minutes – The Preliminary Disturbance Report asks for a preliminary analysis to be conducted regarding the cause of the event – and is still needed. The new report is a compliance document and doesn’t require the same data that is required of the Preliminary Disturbance Report.

The data that is collected in the IROL Violations Report is data that should be readily available to the system operator shortly after an instance of exceeding an IROL. The report doesn’t ask for an analysis, just for a collection of the facts such as what limit was exceeded, how long was it exceeded, etc. The new report must be filed with the compliance monitor within 5 days of the event.



### ***What is an IROL?***

An IROL is a special type of system operating limit. While operating so that system operating limits aren't exceeded is always important, if an IROL is exceeded, there is an increased risk of voltage instability, cascading outages or uncontrolled separation that adversely impacts the interconnection.

System Operating Limits are monitored by system operators working for entities performing the Transmission Operator function and may also be monitored by system operators working for entities performing the Reliability Authority function.

IROLs are monitored by the Reliability Authority. The Reliability Authority may delegate this task to system operators working for entities performing the Transmission Operator function, but it is the Reliability Authority that is held accountable for ensuring that IROLs aren't exceeded.

### ***What is the IROL's $T_v$ ?***

$T_v$  is the maximum amount of time the system operator has to return to a state that is at or below the limit before being subjected to compliance sanctions.

The  $T_v$  associated with each IROL is a time value used to assess how quickly the interconnection may deteriorate if an IROL isn't mitigated. IROLs should never be exceeded – but if one is exceeded, the  $T_v$  represents the maximum amount of time the limit can be exceeded before the risk to the interconnection becomes unacceptable. Under this standard, if a  $T_v$  is exceeded, there are financial penalties and additional reporting requirements.

### ***Why don't all IROL's have the same $T_v$ ?***

The IROL's  $T_v$  is based on system risk – and recognizes that exceeding some IROLs is unacceptable for any length of time, while exceeding other IROLs can probably be tolerated for a longer period of time before there is an unacceptable risk to the interconnection. By establishing a  $T_v$  for each IROL, the RA has information needed to anticipate the negative results of exceeding an IROL. If an IROL can't be exceeded for any length of time, then the RA may choose to install a special protection scheme to control the risk of exceeding the limit in real time. Note that  $T_v$  may not exceed 30 minutes.

### ***If an RA installs a special protection scheme to reduce the probability of exceeding an IROL for time greater than the limit's $T_v$ , does this eliminate the IROL?***

No. The facility being protected by the special protection scheme would still need to be included in the list of facilities subject to IROLs, and the IROL would need to be listed with its  $T_v$ . Since special protection schemes don't always work as planned, it is important that system operators know where they have IROLs, know which facilities are subject to IROLs and know what the  $T_v$  is for each IROL. The system operator needs access to this data to make appropriate system operating decisions when special protection schemes don't work as planned.

### ***How do you develop a list of IROL's?***

The Determine Facility Ratings, System Operating Limits and Transfer Capabilities standard includes a requirement that entities responsible for developing system operating limits document their methodology for developing these limits. The RA is responsible for developing the subset of system operating limits that are called IROLs. The RA must follow its methodology for developing system operating limits and then must identify whether or not exceeding that limit could cause voltage instability, cascading outages, or uncontrolled separation from the interconnected transmission system. If the system operating limit could lead to one or more of these dire consequences, then the limit is an IROL.

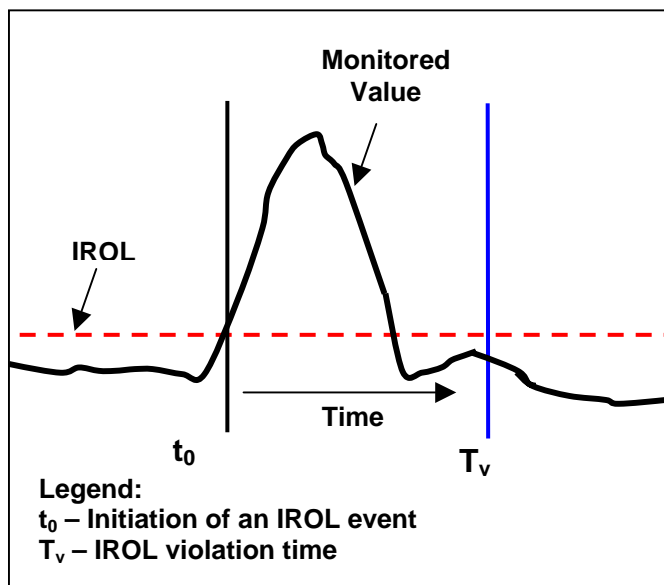
### **How do you establish a $T_v$ for an IROL?**

Each RA may use whatever system it wants for establishing a  $T_v$  for its IROLs. This gives each RA the latitude to be as conservative as it desires. Some RAs may choose to use a default  $T_v$  of 30 minutes – currently some entities have a default of 20 minutes for all limits that would be categorized as IROLs. Here are some ways of setting  $T_v$ :

- Use study results showing the impact of a loss of a unit or line
- Set  $T_v$  at or lower than ‘published’ acceptable time overloads for critical facilities and
- Reference relay settings that have time delays before tripping overloaded facilities

### **Which instances of exceeding an IROL need to be documented?**

All. Every instance of exceeding an IROL for any length of time must be documented. Most entities are expected to document the instance on a system operating log, but the standard does not require that the documentation be on an operating log, just that it be documented.



### **Does the standard require that exceeding an IROL be documented on the system operator’s daily log?**

No. Each entity can document IROL events using whatever documentation system works best for them. While each entity may use whatever system(s) it chooses to document instances of exceeding IROLs, the documentation must be retrievable so it can be shown to the Compliance Monitor. The data can be retrievable through computer screen displays, through paper or electronic logs, or other sources.

### **When you exceed an IROL, what do you have to document?**

When you exceed an IROL for any length of time, you need to document the following three things:

- Actions taken or directives issued
- Magnitude of the event
- Duration of the event

### **How many IROLs do you expect the ‘typical’ RA to have in a year?**

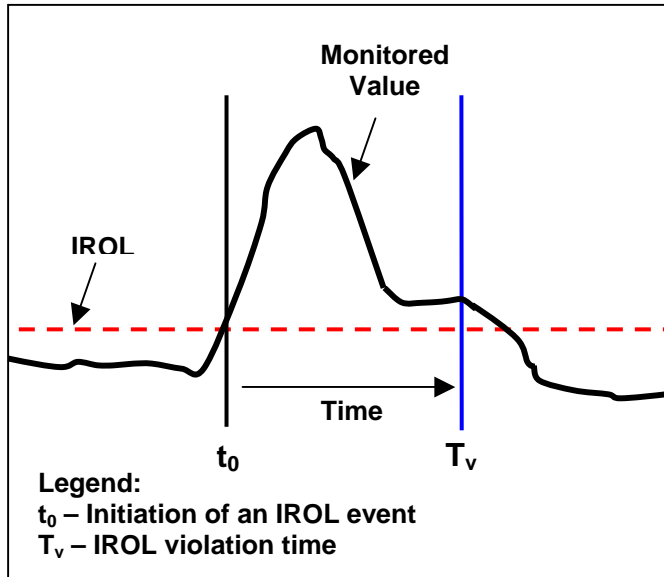
None! This standard focuses on preventing instances of exceeding an IROL. This standard requires the RA to use its tools to actively monitor and assess its Reliability Authority Area with respect to the current

## Questions & Answers About the Operate within IROLs Standard

and expected system conditions. For emerging system conditions, the RA is required to act to prevent exceeding an IROL. For unusual situations, such as a plane crash that knocks down 500kV lines, the RA is required to act to mitigate the instance within the IROL's  $T_v$ . Since most RA's can go many years without ever having a plane crash through their 500kV lines, most RAs won't experience any instances of exceeding an IROL for any length of time.

### **Which instances of exceeding an IROL need to be reported?**

Every instance of exceeding an IROL for time greater than the IROL's  $T_v$  is reported to the Compliance Monitor within five business days.



*The value being monitored exceeded its IROL for a time greater than the IROL's  $T_v$  and the event must be documented **and** reported.*

### **When you exceed an IROL for a time greater than the IROL's $T_v$ , what do you have to report?**

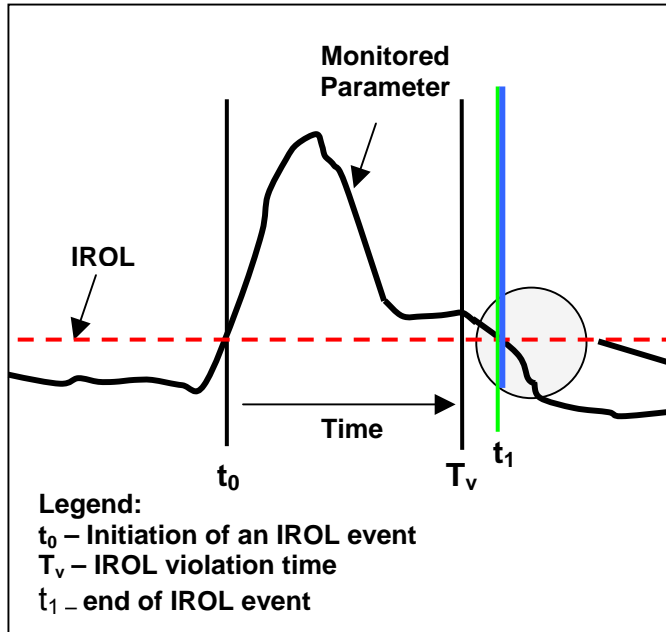
When you exceed an IROL for a time greater than the IROL's  $T_v$ , you have to report the following information to the Compliance Monitor:

- Date and time of the event
- Identification of which interconnection reliability operating limit was violated
- $T_v$  for that limit
- Magnitude and duration of exceeding the interconnection reliability operating limit
- Actions taken or directives issued
- Time actions or directives were initiated or issued,
- Explanation of results of actions or directives

There is a report called the IROL Violation Report that captures this information. This report is available from the NERC Web Site and is provided at the end of this document.

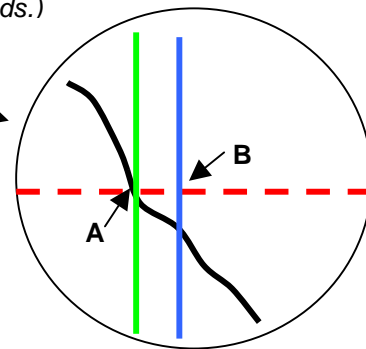
**How do you calculate the duration of an IROL event?**

The duration of an IROL event is measured from the point in time when the IROL is first exceeded to the point in time where the parameter being monitored has returned to a value that is at or below the IROL, providing the actual value remains at or below the IROL for at least 30 seconds.



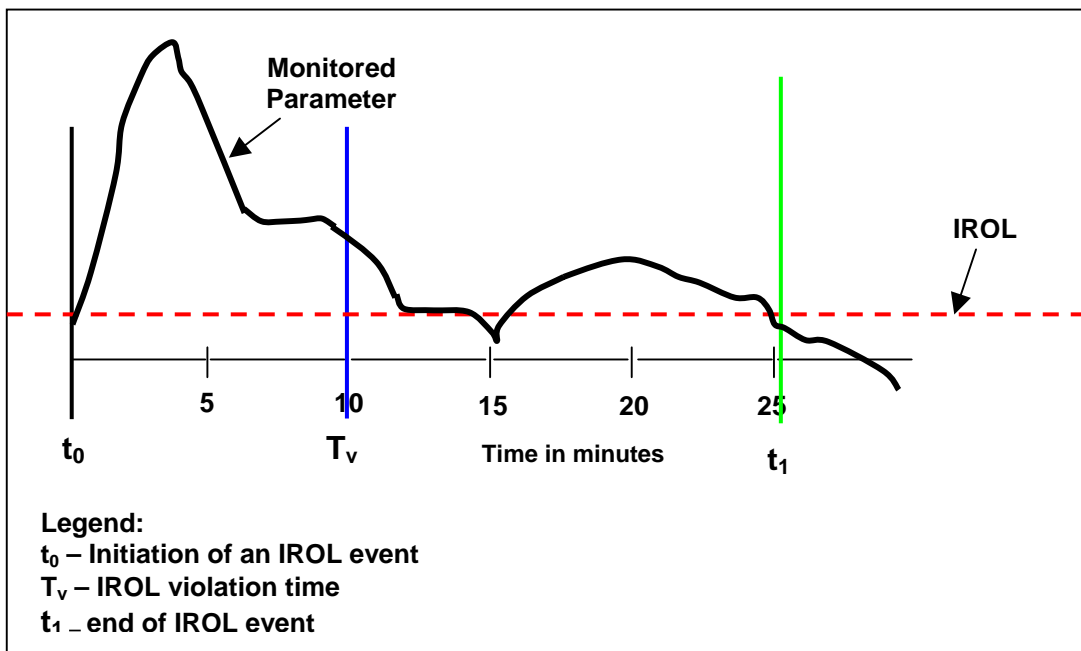
The monitored parameter must remain at or below the IROL for 30 seconds or more.

The line for  $t_1$  shows the end of the IROL event, which is the point in time when the monitored value returns to a value that is at or below the IROL as long as the monitored value remains at or below the limit for at least 30 seconds. (From pt. A to pt. B is 30 seconds.)



The following example is shown in the chart below. The IROL that has been exceeded has a  $T_v$  of 10 minutes. The monitored value exceeds the IROL for 15 minutes, then the monitored value returns to a value that is below that IROL for just 20 seconds, then the monitored value exceeds the IROL for another 10 minutes – then the monitored value returns to a value that is below the IROL for 2 hours. The duration of the event that must be reported is:

- 25 minutes, 20 seconds



## Questions & Answers About the Operate within Operate within IROLs Standard

### *If you exceed an IROL for time greater than $T_v$ , how big is the sanction?*

This is the table used to determine the size of the sanction when an IROL is exceeded for time greater than  $T_v$ .

Example 1: There is an IROL set at 1000 MW with a  $T_v$  of 30 minutes. The IROL is exceeded for 35 minutes. During the time period after  $T_v$  was exceeded (the last 5 minutes of the event), the maximum value was 1100 MW. This is the first IROL violation for this RA.

$$\text{Max Val \%} = (1100 \text{ MW}/1000 \text{ MW} - 1) * 100 = 10$$

The event duration exceeded its  $T_v$  by 5 minutes

The level 4 \$ sanction for the first infraction is \$2000

$$\text{The sanction would be } 10 * \$2000 = \$20,000$$

<b>If the Maximum Value % over the Limit (measured after the event duration exceeds <math>T_v</math>) is:</b> Max Value % = (Max Value/ IROL limit -1)*100	<b>And the event duration exceeds its <math>T_v</math> by ___ minutes:</b>	<b>Then Multiply the Level 4 \$ sanction by:</b>
0% < Max Value % ≤ 5%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	5
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	10
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	15
	$\text{Duration} > T_v + 15 \text{ minutes}$	20
5% < Max Value % ≤ 10%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	10
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	15
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	20
	$\text{Duration} > T_v + 15 \text{ minutes}$	25
10% < Max Value % ≤ 15%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	15
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	20
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	25
	$\text{Duration} > T_v + 15 \text{ minutes}$	30
15% < Max Value % ≤ 20%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	20
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	25
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	30
	$\text{Duration} > T_v + 15 \text{ minutes}$	35
20% < Max Value % ≤ 25%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	25
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	30
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	35
	$\text{Duration} > T_v + 15 \text{ minutes}$	40
25% < Max Value % ≤ 30%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	30
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	35
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	40
	$\text{Duration} > T_v + 15 \text{ minutes}$	45

## Questions & Answers About the Operate within Operate within IROLs Standard

Example 2: There is an IROL set at 1000 MW with a  $T_v$  of 20 minutes. The IROL is exceeded for 35 minutes. During the time period after  $T_v$  was exceeded (the last 5 minutes of the event), the maximum value was 1200 MW. This is the second IROL violation for this RA.

$$\text{Max Val \%} = (1200 \text{ MW}/1000 \text{ MW} - 1) * 100 = 20$$

The event duration exceeded its  $T_v$  by 15 minutes

The level 4 \$ sanction for the second infraction is \$4000

$$\text{The sanction would be } 30 * \$4000 = \$120,000$$

<b>If the Maximum Value % over the Limit (measured after the event duration exceeds <math>T_v</math>) is:</b> Max Value % = (Max Value/ IROL limit -1)*100	<b>And the event duration exceeds its <math>T_v</math> by ___ minutes:</b>	<b>Then Multiply the Level 4 \$ sanction by:</b>
0% < Max Value % ≤ 5%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	5
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	10
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	15
	$\text{Duration} > T_v + 15 \text{ minutes}$	20
5% < Max Value % ≤ 10%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	10
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	15
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	20
	$\text{Duration} > T_v + 15 \text{ minutes}$	25
10% < Max Value % ≤ 15%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	15
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	20
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	25
	$\text{Duration} > T_v + 15 \text{ minutes}$	30
15% < Max Value % ≤ 20%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	20
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	25
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	30
	$\text{Duration} > T_v + 15 \text{ minutes}$	35
20% < Max Value % ≤ 25%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	25
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	30
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	35
	$\text{Duration} > T_v + 15 \text{ minutes}$	40
25% < Max Value % ≤ 30%	$T_v < \text{Duration} \leq T_v + 5 \text{ minutes}$	30
	$T_v + 5 \text{ minutes} < \text{Duration} \leq T_v + 10 \text{ minutes}$	35
	$T_v + 10 \text{ minutes} < \text{Duration} \leq T_v + 15 \text{ minutes}$	40
	$\text{Duration} > T_v + 15 \text{ minutes}$	45

### ***What is the philosophy behind the sanction for exceeding an IROL for time greater than $T_v$ ?***

Most RAs will not exceed an IROL. If there is an ‘emerging’ system condition that is causing operations in the Reliability Authority Area to approach operations outside of the IROLs, then the RA should take actions to prevent the system from exceeding the IROL. This standard requires that the RA monitor and assess its Reliability Authority Area so that emerging system conditions are noted and corrected before an IROL can be exceeded. There are unusual circumstances that do occur – such as a plane crashing through a set of 500 kV lines – that will cause an IROL to be exceeded. When this does occur, the RA needs to take action without delay to remedy the situation. If the RA achieves its goals within  $T_v$ , then there is no sanction.

### ***Why isn't the sanction linked to the highest value over the course of the event?***

Because unusual circumstances occur without warning, the sanction isn't linked to the highest value during the event, the sanction is linked to the highest value during the time period after  $T_v$  has been exceeded. This seemed to be the fairest way of applying the sanction – it gives the RA some time to resolve the situation and allows for ‘credit’ to be given if the RA was able to move the system in the right direction, but wasn't able to achieve the goal of getting within the limits before  $T_v$ .

### ***What's the origin of the concept of these sanctions for exceeding IROLs?***

These sanctions are very similar to the sanctions used for Policy 2 and for the WECC RMS program. The sanction for violating Requirement 204 is linked to the magnitude and duration of the infraction and to the history of the entity with respect to prior similar violations – Policy 2's sanction is linked to magnitude and duration of the infraction and to the size of the company that is responsible for preventing the infraction.

### ***What are you expecting in the requirement for Processes, Procedures or Plans?***

The RA needs to anticipate what actions to take to prevent exceeding IROLs as well as the actions to take when an IROL has been exceeded. The RA has to have some type of document that outlines the actions the RA will take to control the situation. The document can be as specific as needed. It is important that the documents be coordinated with entities that will be involved if the process, procedure or plan is invoked. The Coordinate Operations Standard defines these terms as follows:

**Operating Procedure** – A document that identifies specific steps or tasks that must be taken by one or more specific operating positions to achieve a single specific operating goal. The steps in an Operating Procedure must be followed in the order in which they are presented, and must be performed by the position(s) identified. A document that lists the specific steps to take in removing a specific transmission line from service is an example of an Operating Procedure.

**Operating Process** – A document that identifies general steps for achieving a generic operating goal. An Operating Process includes steps with options that may be selected depending upon real-time conditions. A guideline for controlling high voltage is an example of an Operating Process.

**Operating Plan**- A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.

**IROL Violation Report**

Interconnection Reliability Operating Limit Violation Report Compliance Template			
<b>Entity Performing Reliability Authority Function:</b>			
<b>Report Date:</b>			
<b>Event Date:</b>	<b>Event Start Time:</b>	<b>Event End Time:</b>	
<b>Name of IROL that was exceeded:</b>	<b>Value of the IROL that was exceeded:</b>	<b>The exceeded IROL's T<sub>v</sub>:</b>	
<b>Magnitude of Limit Exceeded after T<sub>v</sub>:</b>		<b>Duration of Event:</b>	
<b>List of Actions Taken or Directives Issued and Results Achieved:</b>			
Time Action Initiated or Directive Issued:	Action Taken or Directive Issued:	Time Action Completed:	Results Achieved:
<b>Report completed by:</b>			
<b>Name:</b>		<b>Phone:</b>	
<b>Title:</b> _____		<b>E-mail:</b>	



When completed, email to: [gerry.cauley@nerc.net](mailto:gerry.cauley@nerc.net)

## Standard Authorization Request Form

Title of Proposed Standard	Operate Within System Operating Limits
Request Date	March 19, 2004

SAR Requestor Information	SAR Type (Put an 'x' in front of one of these selections)	
Name Operate Within IROL SDT; Ed Riley, Chairman of Operate Within IROL SDT	<input checked="" type="checkbox"/>	New Standard
Primary Contact Gerald Rheault, Charles Waits	<input type="checkbox"/>	Revision to existing Standard
Telephone G. Rheault (204) 487-5423 C. Waits (734) 929-1227	<input type="checkbox"/>	Withdrawal of existing Standard
E-mail G. Rheault <a href="mailto:gnrheault@hydro.mb.ca">gnrheault@hydro.mb.ca</a> C. Waits <a href="mailto:cwaits@metcllc.com">cwaits@metcllc.com</a>	<input type="checkbox"/>	Urgent Action

### Purpose/Industry Need (Provide one or two sentences)

The Transmission System must be continuously monitored and assessed to ensure that system operating limits aren't exceeded. Exceeding system operating limits may result in customer outages and equipment damage. This SAR is submitted to establish a standard for data collection, monitoring, and operating within, Transmission System Operating Limits.

### Brief Description

This standard requires monitoring and controlling the transmission system under the authority of the Transmission Operator such that system operating limits are not exceeded.<sup>1</sup> The system operating limits addressed in this standard are established using the methodology defined in Standard 600 and are not the subset classified as Interconnection Reliability Operating Limits in Standard 200.

Requirements shall address:

<sup>1</sup> These are the system operating limits established through the standard, "Determine Facility Ratings, Operating Limits and Transfer Capabilities"

- Real time monitoring of transmission system parameters against system operating limits
- Performing day ahead operational planning analyses and real-time assessments relative to operating within system operating limits
- Keeping the Reliability Authority informed of changes in the status of the transmission system that could affect interconnection reliability
- Keeping the Generator Operators informed of changes in the status of the transmission system that may affect generator operations
- Taking actions to prevent and/or mitigate instances of operating outside system operating limits
- Having and following operating procedures, processes or plans to prevent and mitigate instances of operating outside system operating limits
- Reporting instances of operating outside any system operating limit for more than 30 minutes to the Compliance Monitor

### **Reliability Functions**

<b>The Standard will Apply to the Following Functions</b> <i>(Check box for each one that applies by double clicking the grey boxes.)</i>		
<input checked="" type="checkbox"/>	Reliability Authority	Ensures the reliability of the bulk transmission system within its Reliability Authority area. This is the highest reliability authority.
<input type="checkbox"/>	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within its metered boundary and supports system frequency in real time
<input type="checkbox"/>	Interchange Authority	Authorizes valid and balanced Interchange Schedules
<input type="checkbox"/>	Planning Authority	Plans the bulk electric system
<input type="checkbox"/>	Resource Planner	Develops a long-term (>1year) plan for the resource adequacy of specific loads within a Planning Authority area.
<input type="checkbox"/>	Transmission Planner	Develops a long-term (>1 year) plan for the reliability of transmission systems within its portion of the Planning Authority area.
<input type="checkbox"/>	Transmission Service Provider	Provides transmission services to qualified market participants under applicable transmission service agreements
<input type="checkbox"/>	Transmission Owner	Owens transmission facilities
<input checked="" type="checkbox"/>	Transmission Operator	Operates and maintains the transmission facilities, and executes switching orders
<input checked="" type="checkbox"/>	Distribution Provider	Provides and operates the “wires” between the transmission system and the customer
<input type="checkbox"/>	Generator Owner	Owens and maintains generation unit(s)
<input checked="" type="checkbox"/>	Generator Operator	Operates generation unit(s) and performs the functions of supplying energy and Interconnected Operations Services
<input type="checkbox"/>	Purchasing-Selling Entity	The function of purchasing or selling energy, capacity and all necessary Interconnected Operations Services as required

<input type="checkbox"/>	Market Operator	Integrates energy, capacity, balancing, and transmission resources to achieve an economic, reliability-constrained dispatch.
<input type="checkbox"/>	Load-Serving Entity	Secures energy and transmission (and related generation services) to serve the end user

### **Reliability and Market Interface Principles**

<b>Applicable Reliability Principles</b> <i>(Check boxes for all that apply by double clicking the grey boxes.)</i>	
<input checked="" type="checkbox"/>	1. Interconnected bulk electric systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
<input checked="" type="checkbox"/>	2. The frequency and voltage of interconnected bulk electric systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
<input checked="" type="checkbox"/>	3. Information necessary for the planning and operation of interconnected bulk electric systems shall be made available to those entities responsible for planning and operating the systems reliably.
<input type="checkbox"/>	4. Plans for emergency operation and system restoration of interconnected bulk electric systems shall be developed, coordinated, maintained and implemented.
<input type="checkbox"/>	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk electric systems.
<input type="checkbox"/>	6. Personnel responsible for planning and operating interconnected bulk electric systems shall be trained, qualified and have the responsibility and authority to implement actions.
<input type="checkbox"/>	7. The security of the interconnected bulk electric systems shall be assessed, monitored and maintained on a wide area basis.
<b>Does the proposed Standard comply with all of the following Market Interface Principles?</b> <i>(Select 'yes' or 'no' from the drop-down box by double clicking the grey area.)</i>	
1. The planning and operation of bulk electric systems shall recognize that reliability is an essential requirement of a robust North American economy. Yes	
2. An Organization Standard shall not give any market participant an unfair competitive advantage. Yes	
3. An Organization Standard shall neither mandate nor prohibit any specific market structure. Yes	
4. An Organization Standard shall not preclude market solutions to achieving compliance with that Standard. Yes	
5. An Organization Standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes	

## Detailed Description

The Transmission Operator shall:

- Perform Real-time Monitoring of system parameters against System Operating Limits
  - Monitor parameters that indicate the current state of the local transmission system relative to operating within System Operating Limits
- Perform day ahead Operational Planning Analyses and Real-time Assessments of System Operating Limits
  - Collect data needed to monitor and assess the local transmission system relative to operating within System Operating Limits
  - Conduct Operational Planning Analyses and Real-time Assessments to determine if the local transmission system can be/is being operated within System Operating Limits
- Notify its RA and adjacent TOPs of any changes to the local transmission system that may affect adjacent transmission systems
- Notify Generator Operators of changes to the local transmission system that may affect generator operations
- Act to prevent and/or mitigate instances of operating outside System Operating Limits. These documents shall address the three types of System Operating Limits - thermal, voltage and stability.
  - Have operating processes, procedures or plans for preventing and mitigating instances of operating outside system operating limits
  - Implement operating processes, procedures or plans to prevent or mitigate instances of operating outside system operating limits
  - Define a maximum time  $T_m$  within which the system must be returned to a safe operating mode to a maximum time of 30 minutes.
- Document
  - Log all instances of operating outside system operating limits
  - Report information to the Compliance Monitor based on specified criteria (e.g. magnitude, duration, type of violation, instances of operating outside limits<sup>2</sup>)

---

<sup>2</sup> If an area bounces over a limit, whether it is caused by a contingency or not, this doesn't need to be reported to NERC as long as the area re-prepares within the NERC guidelines. If the NERC criteria are not met, then these violations should be reported.

***Related Standards***

<b>Standard No.</b>	<b>Explanation</b>
600	The Determine Facility Ratings, System Operating Limits and Transfer Capabilities standard identifies how to set System Operating Limits.
200	The Monitor and Assess Short-term Transmission Reliability – Operate Within Interconnection Reliability Operating Limits establishes a subset of System Operating Limits under the control of the Reliability Authority.
	The Transmission Operator Certification standard establishes a list of processes, procedures, tools and agreements that need to be in place before an entity that wants to perform the Transmission Operator function can be certified. This standard assumes that the Transmission Operator has met all criteria required for certification.

***Related SARs***

<b>SAR ID</b>	<b>Explanation</b>

***Regional Differences***

<b>Region</b>	<b>Explanation</b>
ECAR	
ERCOT	
FRCC	
MAAC	
MAIN	
MAPP	
NPCC	
SERC	
SPP	
WECC	

***Related NERC Operating Policies or Planning Standards***

ID	Explanation